FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Firewalls
Sicherheit und Benutzerakzeptanz in Forschungsnetzen

Ralph Niederberger

FZJ-ZAM-IB-9522

September 1995
(Stand 29.9.1995)

Inhaltsverzeichnis

Verzeichnis der Abbildungen

Verzeichnis der Tabellen

1 Einführung

In den letzten Jahren hat das Internet immer mehr an Bedeutung gewonnen. Während anfänglich der Netzzugang ins weltweite Internet im Vordergrund stand, wird heute immer mehr nach der Sicherheit des lokalen Netzes gegen Zugriffe von außen gefragt.

Immer häufiger werden Unternehmen von sogenannten Crackern angegriffen (attack) oder von Cracker-Testprogrammen ausspioniert (probe). Diese Attacken führen zu Durchsatz-, Daten- und Wettbewerbsverlusten (Veröffentlichung geheimer Informationen, Forschungsergebnissen etc.). Angreifer von aussen werden oft Hacker oder Cracker genannt. Da aber das Wort Hacker eher eine positive Bedeutung hat, wird im Folgenden nur der Begriff Cracker benutzt.[1]

Viele Firmen wünschen den Zugang nach aussen oder werden aus wirtschaftlichen Gründen zu diesem Schritt gezwungen. Andere, die seit Jahren bereits am weltweiten Internet angeschlossen sind, erkennen erst jetzt die Gefahren, die sie mit dieser Öffnung nach außen eingegangen sind. Diese Firmen möchten möglichst problemlos alte und auch neue Dienste nutzen können, aber andererseits auch Mechanismen zur Zugangskontrolle von außen zur Verfügung haben. Ein wesentlicher Gesichtspunkt einer solchen Zugangskontrolle ist für diese Unternehmen die Implementierung eines solchen Services in der Art und Weise, daß der normale Benutzer dadurch keine wesentlichen Beeinträchtigungen erfährt, wie z.B. Durchsatzverlust (heutige Firewall-Techniken decken nur Übertragungsraten bis zu 1.5 Mbit/sec ab), zusätzliche Authentisierungsstufen (wie z.B. Anmelden auf einem Gateway-Rechner), Verzögerungen durch Verschlüsselungsmechanismen und durch Logging-Aktivitäten.

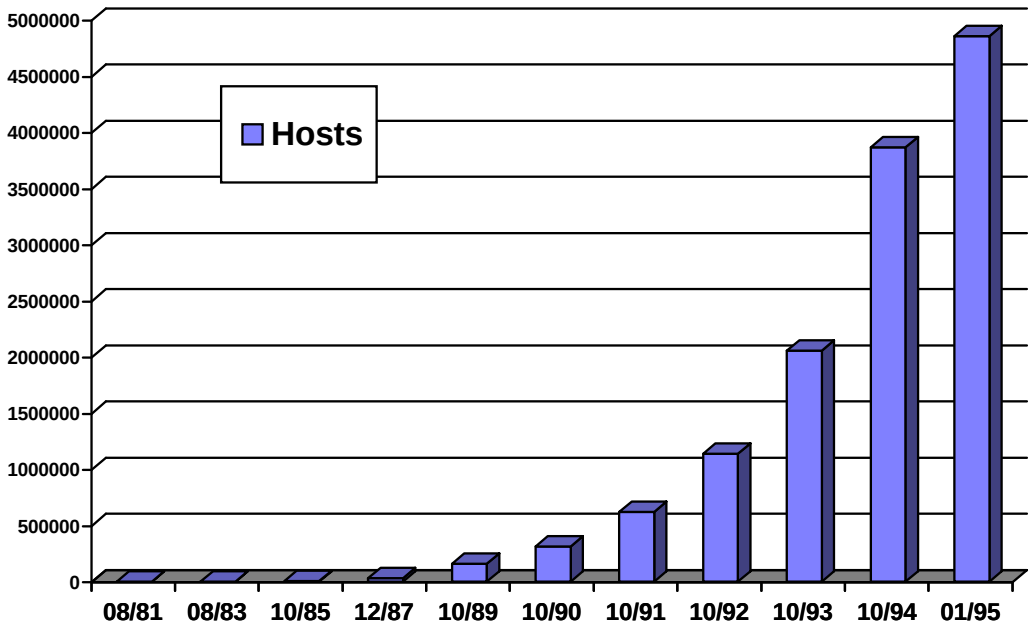


Abb. 1: Benutzerflut:: Anzahl von Rechnern im Internet (1981 — heute)[2]

Firewalls sind hier sicherlich kein Allheilmittel, da sie nur gegen ganz bestimmte Einbruchs- und Sabotageversuche schützen. Als Virenschutz sind sie nicht geeignet.

[1] Hacker sind demgegenüber im allgemeinen Computerbenutzer, die einen großen Teil ihrer Freizeit für Computer verwenden und daher meist auch tiefgehende Kenntnisse im Umgang mit Computern besitzen.

[2] Entnommen aus [Dieth,Haug,Kienle,Heinen], iX-09/95

Ebenso schützen sie nicht vor Innentätern, offene Hintertüren durch Software-Entwickler und Systemadministratoren.

Firewalls sind eine Lösung, um die Vorteile des Internet zu nutzen, ohne die Sicherheitsanforderungen des Unternehmens gänzlich zu vernachlässigen. Sie stellen keinen hundertprozentigen Schutz dar, sondern erhöhen nur die Hürde für potentielle Cracker.

“Why shall the crackers spend 10 minutes here,
when they can take 30 seconds to get in elsewhere?”

Ed DeHart, CERT-USA
Usenix LISA XI — September ’95

Sinn dieser Studie ist, ein generelles Verständnis der Arbeitsweise von Firewalls aufzubauen und auf den Nutzen eines solchen hinzuweisen. In weiteren Abschnitten wird auf die konkrete Situation des Forschungszentrums Juelich, als Beispiel einer Großforschungseinrichtung, eingegangen und eine *Security Policy* entwickelt, die an die Gegebenheiten, Besonderheiten und Anforderungen in der KFA angepaßt ist. Abschließend wird diese *Security Policy* in Hard- und Software implementiert und die Möglichkeit aufgezeigt, wie diese in KFAnet/Internet integriert werden kann.

“A well known site can expect three probes a week — on the average.”

Steve Bellovin, AT&T Bell Labs
Open Computing — October ’94 p83

2.1 Gefahren

Die potentiellen Schwachpunkte, die sich mit dem Anschluß an Internet ergeben, sind leicht zu erklären.

Eine Internet-Anbindung erweitert das lokale Netz um über 70.000 weitere Netze, die an Internet angebunden sind. Die aus der Verbindung nach außen resultierenden Gefahren lassen sich in verschiedene Gefahrenklassen einteilen, die unterschiedliche und teilweise ganz neue Sicherheitsanforderungen an das eigene Netz stellen.

Unterschieden werden muß hier zwischen versehentlichem Agieren und kriminellem Agieren.

Wer kann ermessen wieviele Cracker sich auf den über 5.000.000 Rechnern zu schaffen machen.

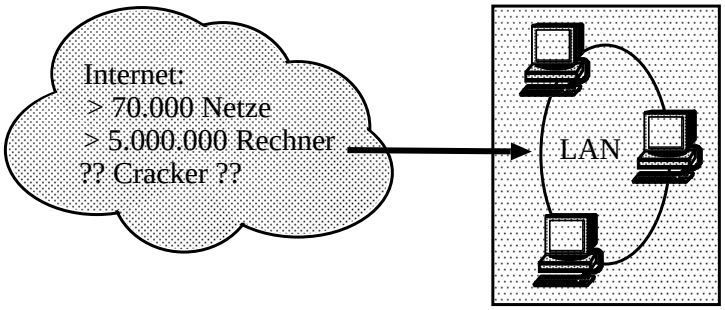


Abb. 2: Netzanbindung und deren Folgen

Die Intention von Crackern läßt sich im Wesentlichen in vier Kategorien einteilen [Robinson, A.T.]:

- Nichtberechtigten Zugriff zu den Ressourcen eines Netzes, z.B. auch um über dieses Netz ein anderes vielleicht lohnenderes Netz zu erreichen.
- Industriespionage oder Erlangen von Geheiminformationen — Im Sinne des Forschungszentrum Jülich eher Forschungsspionage, d.h. gezielte Suche nach z.Zt. geheimer noch nicht veröffentlichter Information.
- Sabotage durch Verursachen finanzieller Schäden, politische Verunglimpfung oder anderweitige Sabotageakte.
- Verbrauch von Ressourcen, um berechtigten Benutzern den Zugriff zu verwehren. (Verbrauch von CPU und/oder Plattenplatz, Netzkapazität, etc.)
  (Denial of Service to legitimate users).

Gefährdet sind somit, die Verfügbarkeit der Systeme und Netzwerke und die auf den Rechnern liegenden Daten. Diese wiederum können kopiert, verfälscht oder gelöscht werden, was im Minimalfall eine Wiederherstellung der Daten durch Backups erfordert. Schwerwiegender wäre z.B. eine Schädigung des Ansehens des Forschungszentrums Jülich, woraus politische und finanzielle Konsequenzen entstehen könnten.

Zur zweiten Kategorie zählen die Gefahren, die aus Unwissenheit oder Neugierde entstehen können:

- Neugierde — Sie richtet zwar keinen Schaden an, kann aber zur Verbreitung sensibler Daten führen, die nicht für die Öffentlichkeit bestimmt waren.
- Versehentliches Offenlegen nicht-öffentlicher Daten (durch z.B. Fehlkonfiguration, falsche Default-Werte bei Systemparametern etc.)

Ziel der Internet Netz Sicherheit ist es, berechtigten Benutzern möglichst freien Zugang sowohl intern als auch extern zu gewähren, jedoch gegen obige Attacken gewappnet zu sein.

Das Internet wurde von Natur aus nicht als sicheres Netz konzipiert. Sinn des Netzes war die leichte Kommunikation ohne große Komplikationen beim Anschluß und der Nutzung. Offener Zugriff für Forschungs- und Entwicklungsaufgaben waren die Haupttriebfedern. Leider hat diese einfache Nutzung auch zu Benutzern geführt, die ethisch andere Gesichtspunkte der Netznutzung in den Vordergrund stellen.

Einfach geschriebene oft Public Domain Software Programme führen zu einem weiteren Schwachpunkt. Die Dienste, die das Internet zur Verfügung stellt, sind teilweise nicht unter Sicherheitsgesichtspunkten geschrieben worden oder enthalten aufgrund ihrer Größe noch unerkannte Sicherheitslöcher.

Ferner ist der größte Teil des Internet-Verkehrs noch unverschlüsselt unterwegs. E-Mail, Passwörter und ganze Dateien können im Fluge mitgelesen werden. Informationen (z.B. Passwörter) hieraus können für spätere Attacken genutzt werden

Ein weiterer Punkt ist die Komplexität der Konfiguration. Viele Organisationen halten es für praktisch unmöglich, ihr weitverzweigtes Netz sinnvoll zu schützen. Da dies scheinbar unmöglich ist, werden keine Sicherheitsüberlegungen getätigt, obwohl dadurch doch wesentliche Verbesserungen erreicht werden könnten.

Ein Irrglaube sollte jedoch so früh wie möglich ausgelöscht werden. Sicherlich kostet Sicherheit eine gewisse Menge an Kommunikationsdurchsatz und erfordert finanzielle Investitionen. Sicherlich läßt sich auch nicht alles so lösen, daß es perfekt ist. Aber das Schließen großer Scheunentore hält zumindest eine Reihe von Crackern ab, weiterzumachen, und alleine das sollte schon die Mühe wert sein.

Eine Hauptgefahr jedoch ist das unterentwickelte Sicherheitsbedürfnis mancher Installationen bzw. mancher System Manager, die weltweit offene Kommunikation zulassen und nicht an die möglichen Gefahren denken. Die meistgenannte Aussage, *wer will den schon was von uns, da gibt es doch lohnendere Ziele und wir haben doch eigentlich nichts zu verbergen*, zeigt deutlich dieses fehlende Sicherheitsbewußtsein. Hier wurde keine *Security Policy* entwickelt, oder besser gesagt eine ganz weit geöffnete *Security Policy*.

Glücklicherweise gibt es jedoch eine Reihe von Lösungsmöglichkeiten, um die Netzsicherheit zu erhöhen. Ein Firewall ist eine dieser Techniken und wird allgemein als sehr effektiv angesehen.

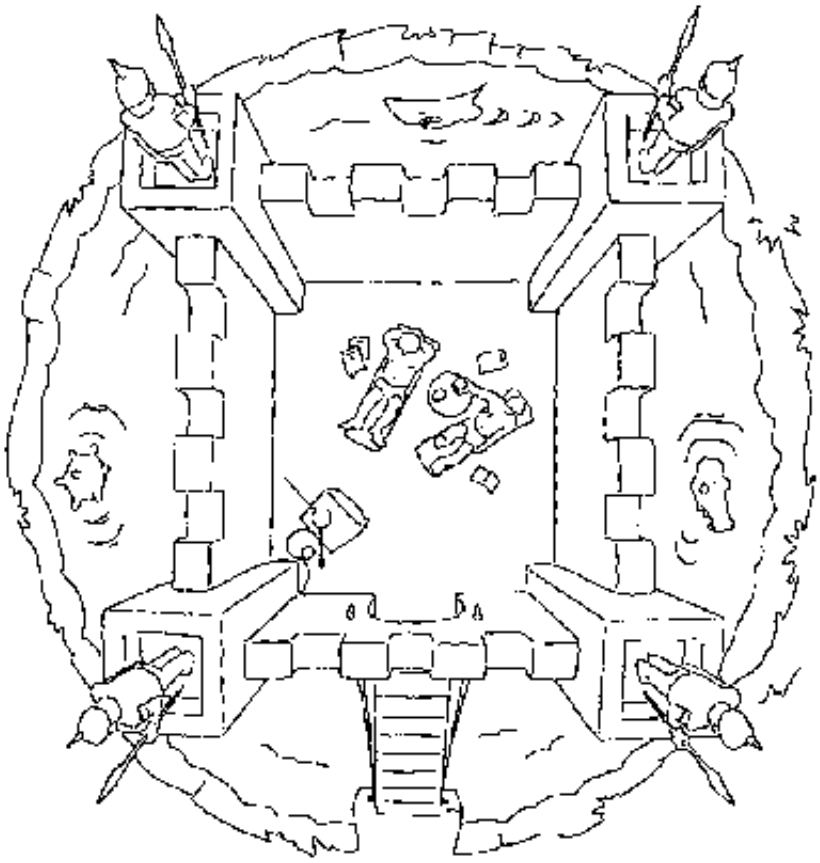


Abb. 3: Firewall, eine Trutzburg gegen externe Gefahren[3]

[3] [Wack,J.P., Carnahan,L.J.]

2.2 Kosten

Firewalls gibt es nicht umsonst. Auch wenn viele Komponenten eines Firewalls eventuell bereits existieren und andere als solche umdefiniert oder umkonfiguriert werden können, gibt es eine Reihe von weiteren Kosten, die bei der Implementation eines Firewalls berücksichtigt werden müssen. Hierbei sind u.a. zu nennen [Cheswick, Bellovin]:

- Hardware-Kosten (inklusive Backup) und Wartung
- Software-Entwicklung und Wartung
- Software-Update-Kosten
- Administrative Kosten für Setup und Training
- Fortlaufende Administration und Problemlösung
- Gewinnverluste, bzw. Verbindungsverlust aufgrund eines fehlerhaften oder defekten Firewalls
- Verlust von Services, die ohne Firewall eventuell angeboten würden, bzw. benutzt würden

Diese Kosten müssen den Kosten gegenübergestellt werden, die entstehen, wenn kein Firewall zur Verfügung steht, als da wären:

- Aufwand der zu treiben ist, wenn eine Attacke stattgefunden hat
- Wiederherstellen verlorengegangener Dateien (Forschungsergebnisse von Jahren?)
- Kosten der Rechner und Netzkapazität, die von Crackern genutzt wird
- u.a.

Diese Kosten variieren natürlich von Organisation zu Organisation, sind aber nicht vernachlässigbar klein.

"Security takes as much time as you put into it.
Security costs as much as you are willing to spent for it.
You will get as much security as you intend to invest for it"

Allgemein anerkannte Statements
Überall nachzulesen

3.1 Allgemeines zum Firewall

Da für den Bereich der Firewalls eine Reihe von einführender Literatur existiert, die ausführlich auf die Vor- und Nachteile der verschiedenen Konzepte eingeht, soll an dieser Stelle auf eine ausführliche Diskussion der unterschiedlichen Konzepte verzichtet werden. Hier seien nur die wesentlichen Begriffe nochmals kurz erklärt.

Ein **Internet Firewall** ist die Implementierung einer Security Policy eines Unternehmens in Form einer Gateway-Maschine, eines Routers oder einer Kombination aus beidem. Es gibt sehr viele unterschiedliche Typen und Techniken der Implementierung von Firewalls. Welcher Typ für das einzelne Unternehmen der beste ist, hängt von sehr vielen Faktoren ab.

Ein Firewall impliziert ein sicheres Netzwerk im Innern und ein weniger sicheres Netzwerk extern.

Internet Zugriff von außen nach innen führt zu reduzierter Sicherheit im Innern auf den gleichen Sicherheitslevel wie außen, entsprechend dem Netz vertrauenswürdiger Rechner.

Zonen eines lokalen Netzes mit unterschiedlichen Security Policies erfordern einen Firewall zwischen diesen Zonen. In jeder Zone kann es nur eine Security Policy geben.

Derzeit ist der beste Weg sicheren offenen Internet Zugang zur Verfügung zu stellen, durch sogenannte Puffer-Netzwerke mit mehr oder weniger offenen Rechnern vor dem Firewall.

Firewall Architekturen können in vier Klassen eingeteilt werden [Ellermann,U. – 1]:

- Packet Screens
- Gateways
- Kombination von Packet Screen und Bastion
- Mischtechniken.

3.2 Packet Screen

Eine **Packet Screen** ist ein Router, der zwischen lokalem Netz und weltweitem Internet, nur Pakete durchläßt, die aufgrund seiner Konfiguration zugelassen sind. Andere Namen für Packet Screens sind **Screening Router** oder **Packet Filter**. Im folgenden wird der Begriff Packet Filter jedoch, wie allgemein üblich, als die Menge der Filter Regeln verstanden, die in einem Router konfiguriert sind. Genau genommen wird eine Packet Screen durch Packet Filter im Router implementiert.

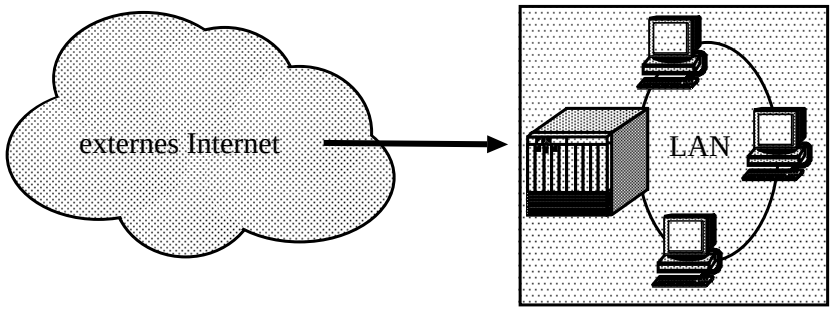


Abb. 4: Netzanbindung durch Packet Screen

Mit neueren Routern können Packet Filter so definiert werden, daß abhängig von

- dem Interface, auf dem das Paket ankommt
- der Source IP Adresse
- dem Source TCP/UDP Port
- dem Interface, für das das Paket bestimmt ist
- der Ziel IP Adresse
- dem Ziel TCP/UDP Port
- dem Protokol (TCP/UDP/ICMP)
- dem Verbindungszustand (ACK Bit gesetzt)
- den IP Optionen

Pakete zugelassen oder abgewiesen werden können.

Packet Screens müssen demnach die einzelnen Pakete Netzwerk- bzw. Transportebene überprüfen.

In das ISO-Referenz-Modell können Packet Screens demnach wie folgt eingruppiert werden:

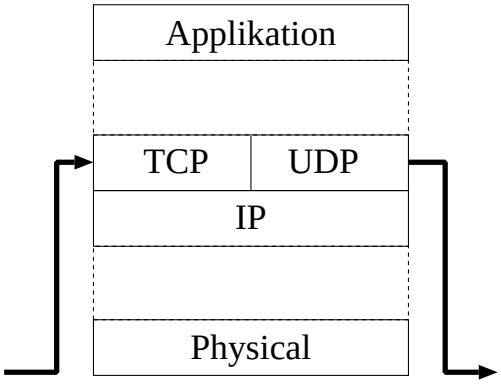


Abb. 5: Die Packet Screen im ISO-OSI-Referenz-Modell

Bei Packet Screens gibt es im wesentlichen zwei Arten von Security Policies, die natürlich jeweils in abgewandelter Form vorkommen können. Diese sind:

Alles das, was nicht ausdrücklich verboten ist, ist erlaubt.

Alles das, was nicht ausdrücklich erlaubt ist, ist verboten.

Welche der beiden Policies angewendet wird, ist von der Gesamtsituation eines Unternehmens abhängig.

3.3 Gateway

Ein Rechner, der Verbindung zu zwei verschiedenen Netzen hat, wird als Gateway bezeichnet, wenn Verbindungen, die über den Rechner laufen, auf Applikationsebene realisiert werden. Wird dieses Gateway dann mit ausführlichem Audit versehen, so kann es als Firewall genutzt werden.

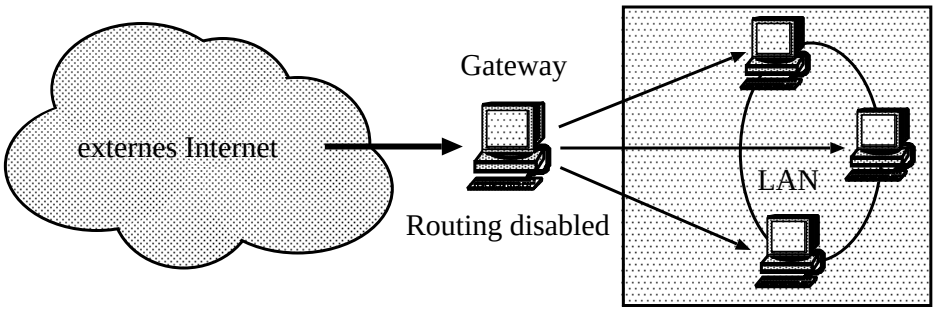


Abb. 6: Netzanbindung durch Gateway (logische Sicht)

Wesentlich für das Gateway ist die Abschaltung des IP-Forwarding, also die Fähigkeit, IP-Pakete zu *routen*. Hierdurch ist keine direkte Verbindung auf IP-Ebene zu einem anderen externen Netz mehr möglich. Der einzige vom Internet aus erreichbare Rechner ist das Firewall-Gateway und Verbindungen sind nur noch über auf dem Gateway installierte Applikationen möglich.

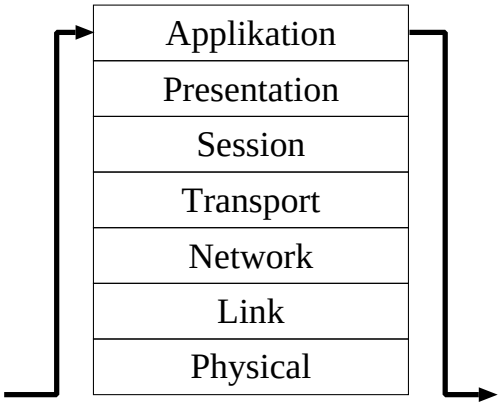


Abb. 7: Die Packet Screen im ISO-OSI-Referenz-Modell

Die Implementierung eines Gateway Firewalls kann auf mehrere Arten geschehen. Die einfachste und reinste Form ist die in der folgenden Abbildung dargestellte. Das Gateway wird hier als Dual-homed Gateway-Firewall bezeichnet.

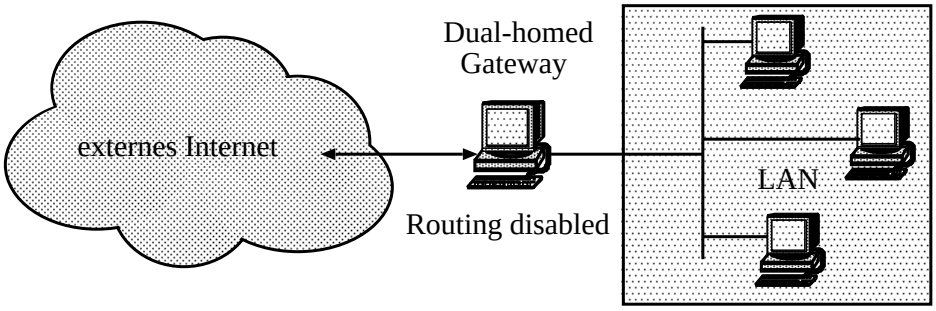


Abb. 8: Netzanbindung durch Gateway (Dual-homed)

Andere Formen sind logisch gleichwertig, jedoch physikalisch anders realisiert. So kann man ein Gateway auch mit einem Interface betreiben. Alle internen Rechner haben keine expliziten Routes nach draußen, d.h. der Default-Route geht zum Firewall-Gateway. Da hier Routing abgeschaltet (disabled) ist, können keine Pakete nach außen gelangen. Externe Verbindungen gehen als Applikationen oder per Proxy-Service über das Gateway nach außen.

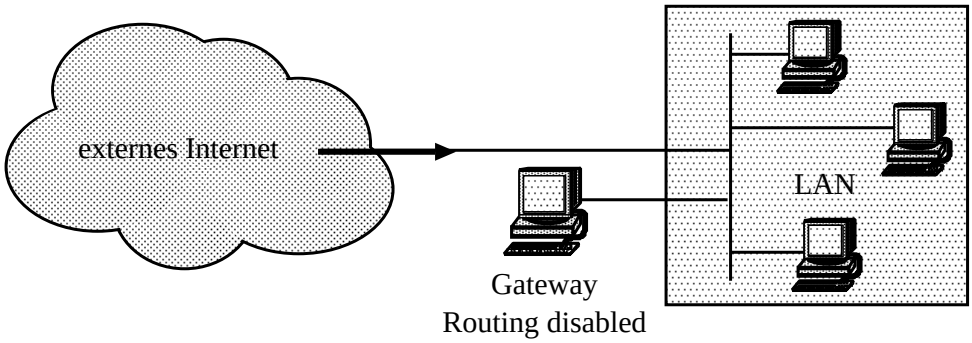


Abb. 9: Netzanbindung durch Gateway (Single-homed)

Einen Firewall auf Basis eines Gateways zu errichten, bietet sich eigentlich derzeit nur für kleinere lokale Netze mit relativ geringer Anbindungsgeschwindigkeit an das externe Internet an, die bereits heute auf der Basis eines Unix-Rechners angeschlossenen sind. Anbindungen durch Firewall–Gateways, die Durchsatzraten über T1 erreichen, sind in der einschlägigen Literatur bisher nicht bekannt geworden.

Einfach ist dies für Applikationen wie Mail und NetNews, die nicht zeitkritisch sind und nach dem Store- und Forward-Prinzip arbeiten. Schwieriger wird es schon für Telnet. Für FTP muß dieses Gateway dann aber bereits so leistungsfähig sein, daß dies für die zukünftigen Netzbandbreiten mit heutigen Workstations nicht mehr oder nur sehr teuer realisierbar ist. Für kleinere Installationen mit geringerer Anforderung an Bandbreite kann das Gateway auf zwei Arten realisiert werden. Erstens kann für die Benutzer, die diesen Service nutzen wollen, ein Account auf dem Gateway eingerichtet werden (*Applikation-Level-Gateway*). Dieser Ansatz sollte nicht implementiert werden, da hierdurch das Applikation-Gateway wieder angreifbar wird. Zweitens können auf

dem Gateway sogenannte Proxy-Server installiert werden (*Circuit-Level-Gateway*). Ein Proxy-Server nimmt Verbindungen vom Quellrechner an, und leitet diese zum Zielrechner quasi transparent weiter. Zwischenzeitlich kann er Quell- und Zieladressen überprüfen, Audit machen und zusätzliche Security-Überprüfungen (Audit) durchführen.

Wird ein Proxy-Server in einem Firewall installiert, so muß eine Client-Anwendung zuerst Kontakt mit dem Firewall aufnehmen. Der Proxy-Server überprüft nun zuerst die Authorisierung des Benutzers. Anschließend wird nach dem zu kontaktierenden Rechner gefragt. Nachdem dieser Rechner vom Benutzer angegeben wurde, verbindet sich der Proxy-Server mit dem entfernten Rechner. Nun wird die gewünschte Funktion durch den Proxy-Server quasi durchgeschaltet. Das ganze läuft also in zwei logisch voneinander getrennten Schritten ab.

- Der Workstation-Benutzer startet z.B. den Telnet oder FTP Client und verbindet sich mit dem Proxy-Server auf dem Firewall.
- Der Proxy-Server schaltet die authorisierte Telnet- oder FTP-Verbindung zu dem entfernten Rechner durch. Der Datenverkehr findet dann transparent über den Proxy-Server statt.

Eine Durchsatzerhöhung kann erreicht werden, wenn mehrere Gateways parallel für die verschiedenen Applikationen zur Verfügung gestellt werden.

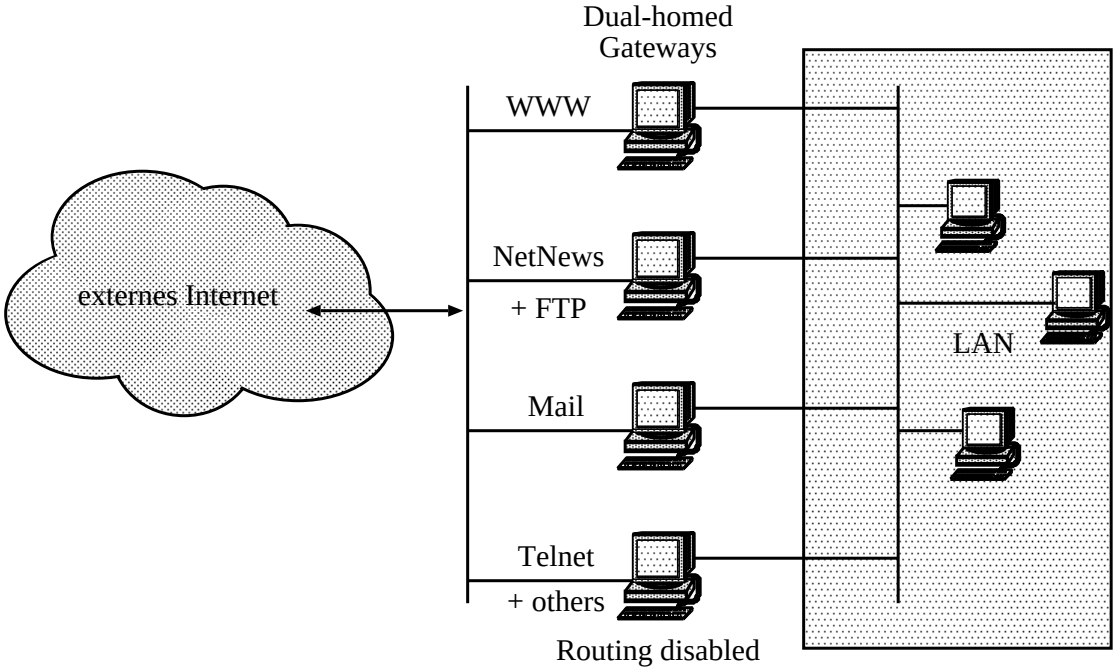


Abb. 10: Netzanbindung durch ein Gateway—Cluster (Beispiel)

Für die KFA scheint eine Anbindung über ausschließlich ein oder mehrere Applikation- oder Proxy-Gateways undenkbar, da hiermit kein ausreichender Datendurchsatz erreicht werden kann. Ca. 2500 Rechner mit potentiell 4500 Benutzern, die teilweise extern kommunizieren, können auch durch ein leistungsfähiges Applikation-Gateway nicht ausreichend unterstützt werden.

Hier müssen andere Konzepte im Hinblick auf Performance und Ausfallsicherheit eingesetzt oder zum Beispiel eine Strukturierung nach Diensten durchgeführt werden.

3.4 Kombination von Packet Screen und Bastion

Bringt man die beiden bisherigen Konzepte zusammen, so gelangt man zu einem komplexeren Firewall.

An dieser Stelle soll der Begriff Firewall, der bisher in allgemeiner Natur benutzt wurde etwas ausführlicher und konkreter gefaßt werden.

Ein *Firewall* besteht aus verschiedenen unterschiedlichen Komponenten. Zum ersten blockieren die Filter, *packet filters*, Übertragungen bestimmter Verkehrsklassen. Das (Applikation-)Gateway ist ein oder eine Menge von Maschinen, die die Applikationsdienste zur Verfügung stellen, und somit quasi eine Ausnahme (bzw. Umgehung) zu den Filterregeln darstellen. Das Netzwerk, an welches das oder die Gateways angeschlossenen sind heißt *demilitarisierte Zone (DMZ)*. Oft gibt es zu den Applikation-Gateways noch ein internes Gateway oder einen internen Router, der die demilitarisierte Zone vom lokalen Netz abtrennt. Meist wird das Applikation-Gateway aufgrund seines Sicherheitsbedürfnisses an exponierter Stelle auch als *Bastion (oder bastion host)* bezeichnet. Dieser Rechner wird mit ausführlichem Audit, Access-Control und möglichst sicherer Software bestückt. Sichere Software heißt in diesem Zusammenhang, ausschließlich Software, die leicht überschaubar (wenig Code) und funktional auf die notwendigen Funktionen beschränkt ist, sowie auf mögliche Sicherheitslücken untersucht wurde.

Die Packet-Screen sorgt dafür, daß alle Verbindungen über die Bastion geführt werden. Hierbei können verschiedene Konzepte, abhängig von der Position der Bastion im Netz unterschieden werden.

InnerBastion: Die Bastion liegt im LAN und ist von diesem leicht zu erreichen. Der Router beschränkt den Zugriff vom Internet auf diesen Host. (Nach [Ranum 92b] auch *Screened Host*)

MiddleBastion: Die Bastion hängt an einem eigenen Netzstrang, zu dem der Zugang sowohl vom Internet als auch vom LAN aus durch einen Router beschränkt wird. Dieses Konzept kann man mit einem oder zwei Routern implementieren.

OuterBastion: Die Bastion hängt an einem eigenen Netzstrang, der vom Internet aus unbeschränkt erreichbar ist. Die Hosts am LAN können im Internet, beschränkt durch den Router, nur die Bastion erreichen.

MiddleBastion und OuterBastion werden nach [Ranum 92b] auch als *Screened Subnet* bezeichnet.

3.4.1 InnerBastion

Eine InnerBastion wird realisiert, indem man den meist bereits vorhandenen Router zum externen Netz als Packet Screen ausbaut und Datenverkehr von und nach außen nur noch über die Bastion zuläßt. Im Router werden hierzu entsprechende Packet Filter definiert (Access Lists im Cisco-Jargon). In der *reinen Lehre* sind hierdurch keine Anwendungen mehr möglich, für die die Bastion kein Applikation- bzw. Proxy-Gateway zur Verfügung stellt (, da IP-Forwarding abgeschaltet).

Aufgrund unterschiedlicher Definitionsmöglichkeiten der Packet Filter im Router kann dieses Konzept beliebig aufgeweicht werden. So können bestimmte Ports freigeschaltet

werden, um direkte Kommunikation zuzulassen. Es kann vereinbart werden, daß nur Verbindungen von innen nach außen initiiert werden können etc. Der Vielfalt von Konfigurationsmöglichkeiten sind quasi keine Grenzen gesetzt. Einschränkungen ergeben sich eigentlich nur durch die Komplexität der Konfiguration (unüberschaubar, fehleranfällig). Eine Beispielkonfiguration zeigt das folgende Bild:

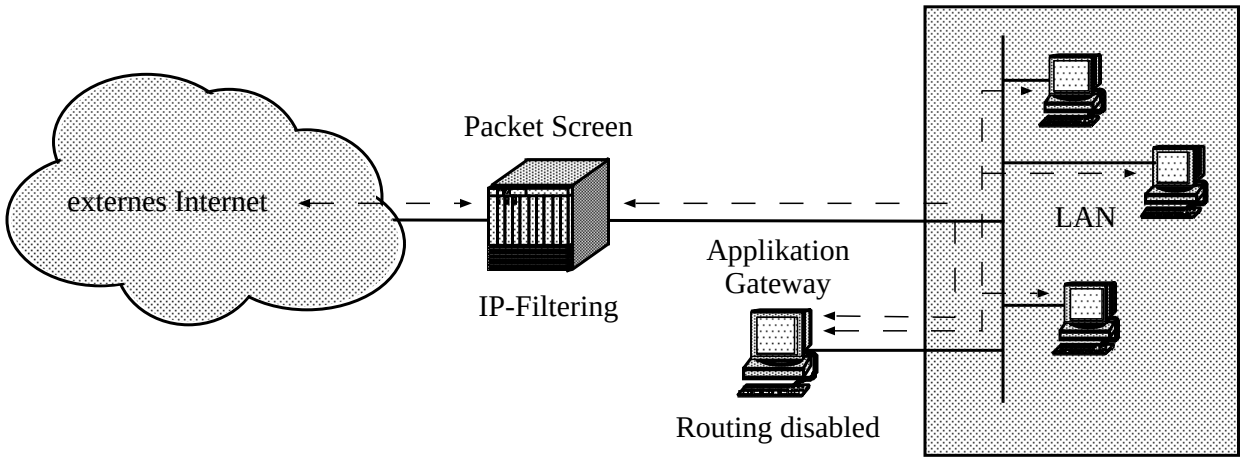


Abb. 11: Netzanbindung durch InnerBastion (Schema)

3.4.2 MiddleBastion

Die Konfiguration eines Firewalls mit InnerBastion hat einige Nachteile.

Angriffe auf die Packet Screen können nicht mitgeschnitten werden, da die Pakete nicht die Bastion erreichen. Kann ein Angreifer von außen die Paket Filter umdefinieren, so gehen die nachfolgenden Pakete an der Bastion vorbei.

Ferner können Insider, also Administratoren lokaler Rechner als Source-Adresse die Adresse der InnerBastion vortäuschen und somit diese umgehen. Man spricht hier von einem Innentäter-Modell. Auf das Innentäter-Modell wird jedoch im weiteren nicht eingegangen. Einen Schutz dagegen erhält man jedoch durch die Konfiguration einer sogenannten *MiddleBastion*.

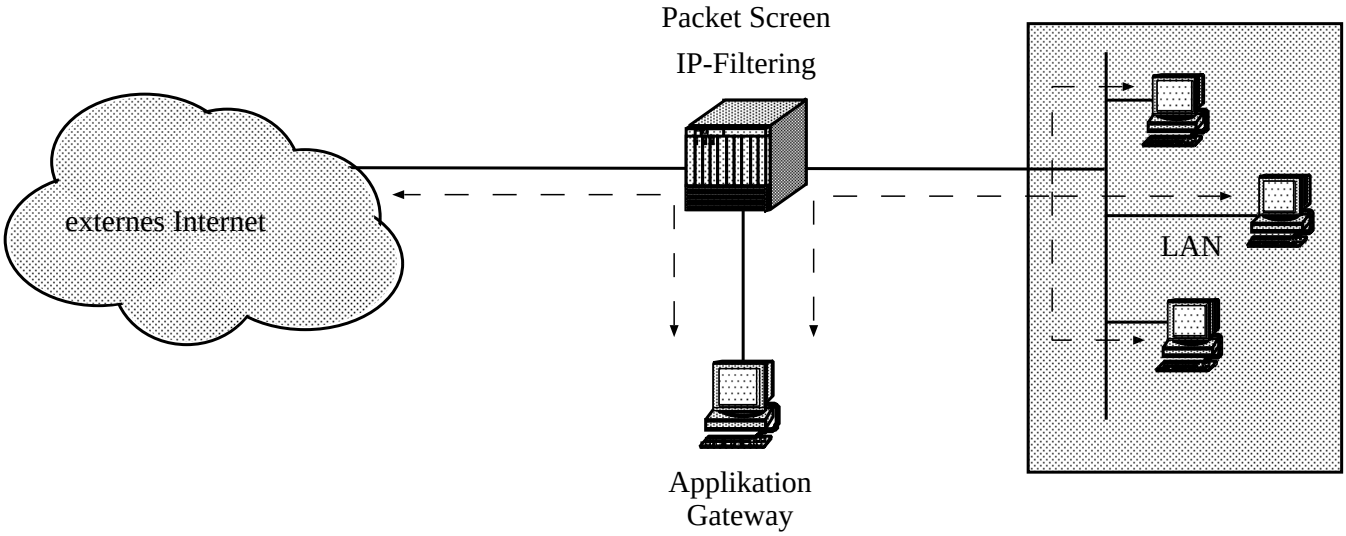


Abb. 12: Netzanbindung durch MiddleBastion (Schema)

Bei der MiddleBastion liegt die Bastion an einem eigenen Netzstrang. Pakete kommen ausschließlich von der Packet Screen zur Bastion. Vortäuschen falscher Adressen durch Innentäter ist nicht möglich. Filter auf der Packet Screen können nun erkennen, über welches Interface Pakete mit der Adresse des Firewall-Subnetzes kommen, und können diese falschen Pakete vernichten.

Wird auf die Definition von Filtern verzichtet, so landen Pakete aus dem Internet, die an das Firewall gerichtet werden, immer im Subnetz der Bastion. Auch hier kann also keine Kommunikation mit internen Rechnern zustandekommen. Es handelt sich somit um einen sehr sicheren Firewall, der allerdings den Nachteil eines geringeren Durchsatzes beinhaltet. Jedes Paket über die Bastion wird zweimal auf das Firewall Subnetz geschickt.

3.4.3 OuterBastion

Den Nachteil, daß Angriffe auf die Packet Screen nicht erkannt werden, kann man durch eine OuterBastion ausschalten.

Hier liegt die Bastion vor der Packet Screen, d.h. jedes Paket, das über die Packet Screen geht, kann auf dem Netz mitgeschrieben und gegebenenfalls analysiert werden. Bei diesem Konzept muß vor den Firewall noch ein zusätzlicher Router geschaltet werden, der die externen Pakete weiterleitet. Dieser Router enthält keine Filterregeln, d.h. alle Pakete können ihn ungehindert passieren. Demzufolge muß ein besonderer Augenmerk auf den Schutz der Bastion gelegt werden.

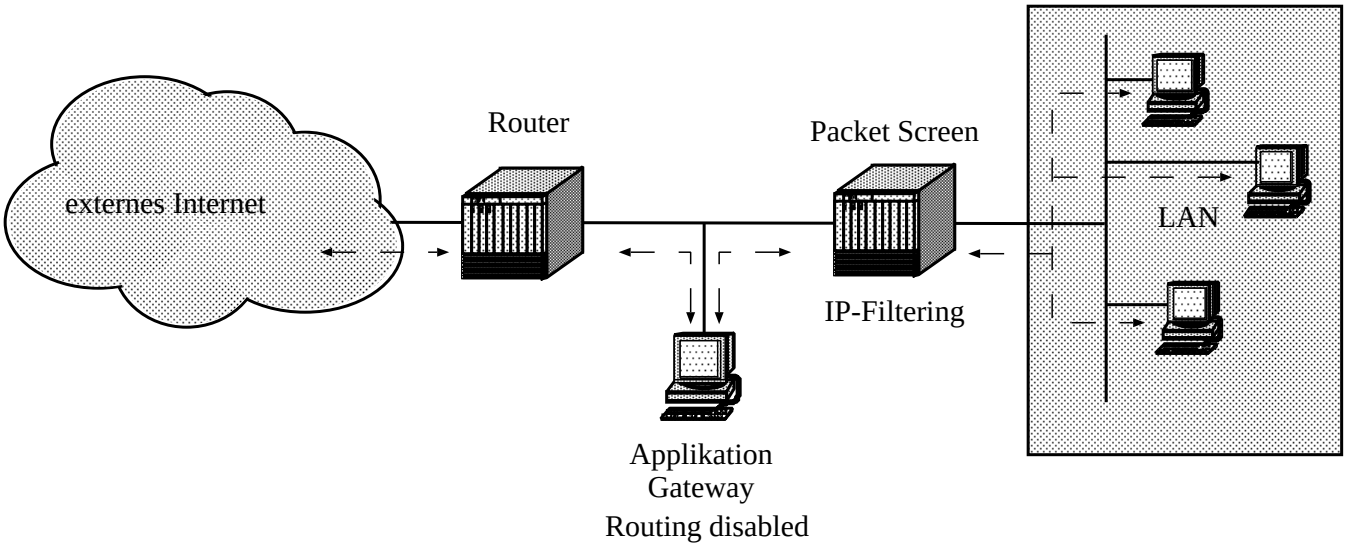


Abb. 13: Netzanbindung durch OuterBastion (Schema)

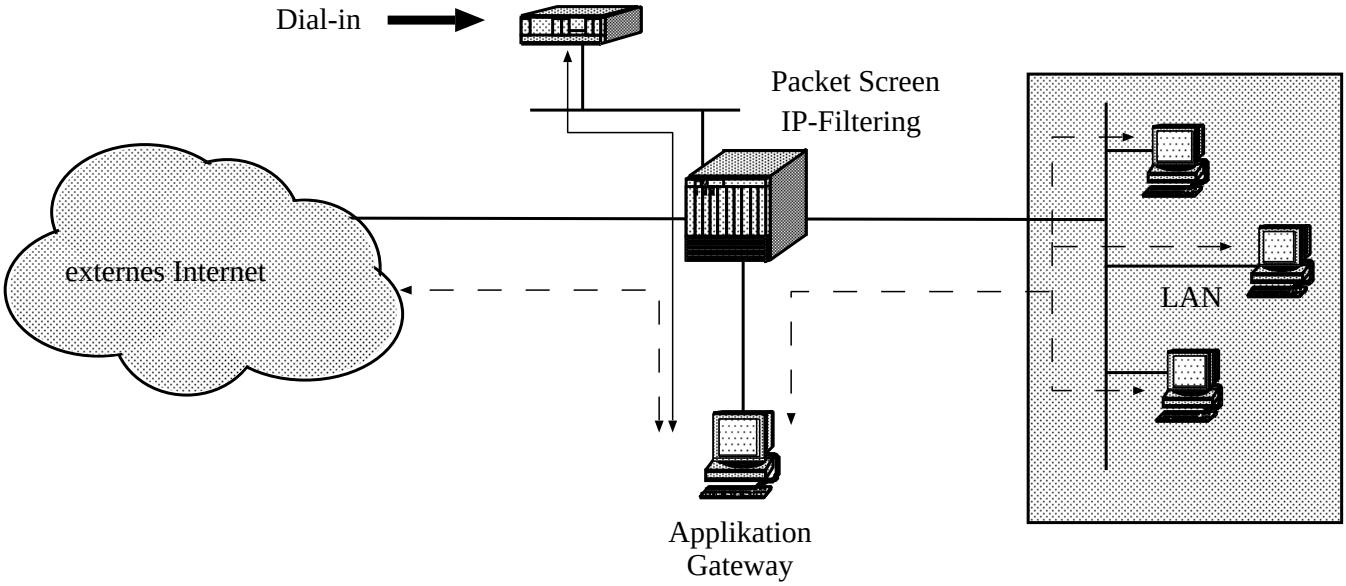
3.5 Mischtechniken

Auf Mischtechniken soll hier nicht eingegangen werden. Sie ähneln in der Struktur im wesentlichen den bereits hier aufgezeigten, enthalten aber weitere Sicherheitsmassnahmen, besondere Vernetzungstechniken, Monitoring, Tunnelingtechniken, etc. Zu den Mischtechniken gehört u.a. das AT&T Firewall [Cheswick, Bellovin], welches als historisch gewachsenes Firewall als klassisches Beispiel einer Mischtechnik angesehen werden kann.

3.6 Integration von Modems in ein Firewall-Konzept

Viele Einrichtungen bieten externen Zugang über Modems an. Für ein Firewall-Konzept stellen diese eine Hintertür und somit ein potentielles Sicherheitsrisiko dar.

Eine bessere Lösung stellt hier eine Konzentration dieser Modems in einen Modem-Pool dar. Hierzu können die Modems auf einen Terminal-Server konzentriert oder zumindest in einem separaten Subnetz zusammengefaßt werden. Zugang zum internen Netz kann dann entweder direkt gewährt werden, wenn der Modem-Zugang als sicher angesehen werden kann, oder indirekt über einen weiteren Sicherheitsmechanismus (z.B. besondere zusätzliche Passwort-Abfrage oder durch Einloggen auf einem Gateway-Rechner.



Die obige Abbildung zeigt, daß unter diesen Voraussetzungen ein Modem-Pool wie ein Zugriff aus dem externen Internet behandelt werden kann. Wird der Modem-Pool außerhalb des Firewalls installiert, können auf dem Applikation-Gateway zusätzliche Authentisierungsmechanismen angezogen werden. Das Packet Filtering System kann Verbindungen interner Rechner zum Modem-Pool einschränken oder verhindern. Durch Abkapselung des Subnetzes auch vom externen Internet schützt der Packet Filter auch den Modem-Pool vor Zugriffen von außen.

4 Die KFA im Internet heute

TCP/IP stellt heute das am meisten benutzte Netzwerk Protokol im wissenschaftlich technischen Bereich in der KFA dar. EARN/Bitnet hatte im lokalen Bereich praktisch keine Bedeutung, Die DECNET—Nutzung stagniert, bzw. ist durch die kontinuerliche Ablösung der VAX-Architektur durch leistungsfähige RISC-Architekturen im DEC Bereich rückläufig.

Derzeit sind auf dem Gelände der KFA ca. 3000 Rechner vom Entry-Level-PC bis zu den Super-Computern, CRAY YMP, CRAY M/94 und Intel Paragon installiert und an KFAnet/Internet angeschlossen.

Haupttransportmedium ist derzeit FDDI mit 100 Mbits/s zu den KFA Instituten mit hohen Brandbreiteanforderungen und Ethernet mit 10 Mbit/s andernfalls. ATM ist in der Planung, Vorbereitung und Testphase.

Die derzeit zur Verfügung gestellten Netzwerkdienste sind FTP, Telnet, Elektronic Mail, Line Printing, Sun's NFS, NetNews und WWW. Weitere Applikationen, basierend auf dem BSD Socket Interface, sind in Benutzung.

Für Backup und Archivierung wird ADSM (ADSTAR Distributed Storage Manager) benutzt.

Durch die Einführung der TCP/IP Protokollfamilie wurde die Möglichkeit eröffnet, leistungsfähige Workstations in Verbindung mit den existierenden Großrechnern zu Nutzen (Workstationkonzept). Durch dieses Konzept konnte

- die Produktivität der Benutzer gesteigert,
- die technische Infrastruktur ausgebaut (die Angebote sind *state of the art*)
- neue Computing Konzepte getestet und realisiert
- die zentralen Dienste und Ressourcen effektiver und ökonomischer genutzt

werden.

Die Öffnung der KFA in Richtung TCP/IP kann als gelungen angesehen werden, was, wie zu erwarten war, an den Wachstumsdaten sowohl intern als auch extern installierter Systeme im TCP-Bereich erkennbar ist. Dieses Wachstum, in dem Bestreben der maximalen und einfachen Konnektivität, lies leider den Sicherheitsgesichtspunkt außer acht. Passwörter gehen unverschlüsselt weltweit über die Netze. Wenn auch auf den meisten Kommunikationspfaden ein Abhören unwahrscheinlich, weil technisch zu aufwendig ist, sollte man die Möglichkeit, daß Daten abgehorcht werden können nicht außer acht lassen. Große Programmprodukte enthalten nach einer allgemeinen Schätzung auf je 1000 Zeilen Assembler Code ca. 1 Fehler. Diese Fehler werden meist irgendwann entdeckt und behoben. Aber immer wieder treten Fälle auf, bei denen man durch falsche Benutzung eines Produktes (falsch im Sinne von *nicht vorgesehen*) Privilegien (z.B. *Root-Privileg*) erhält, die vom Programm-Schreiber nicht gewünscht waren.

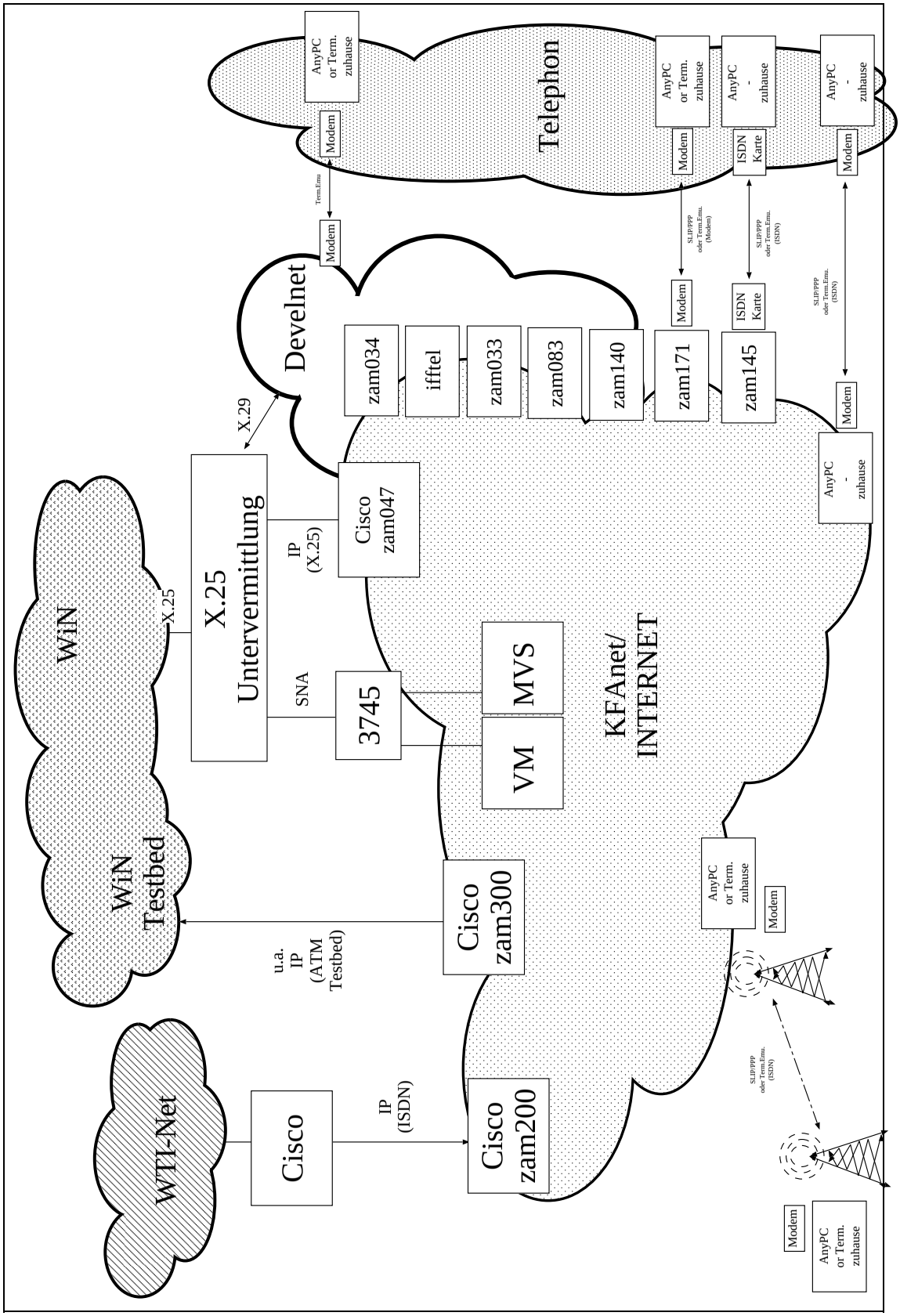


Abb. 14: Wege in die KFA heute

Das Erlangen der Super-User-Rechte auf einem Unix-System betrifft nicht nur diese eine Maschine. Durch die Netzwerkverbindung dieser Maschine mit anderen, sei es durch

.rhosts, host.equiv Dateien, Network File System, Dateien mit enthaltenen Passwörtern anderer Rechner[4] etc., kann dieser User wiederum Berechtigungen auf anderen Rechnern erhalten. Ein sogenanntes *Net of Trust* bricht zusammen.

Was dies für ein lokales Netz bedeuten kann ist eindeutig. Verläßt man sich auf die Sicherheit eines Rechners im Netz, so verläßt man sich automatisch auch darauf, daß alle ihm vorgeschalteten (vertrauenswürdigen) Rechner ebenfalls sicher sind. Dies muß im allgemeinen angezweifelt werden. Wie aber läßt sich ein Netz sicher machen.

Ein Weg ein Netz sicher zu machen, ist die Sicherheit auf allen angeschlossenen Rechnern zu erhöhen. Einige der notwendigen Maßnahmen sind:

- Durchsetzen von *strong passwords*: Die meisten Systeme erlauben dem Benutzer einfache Passwörter ohne Sonderzeichen und ohne Ziffern zu spezifizieren. Dies führt zu Passwörtern, die leicht zu erraten sind und dann meist auch noch nicht in gewissen Abständen geändert werden müssen. Oft kann durch Eingabe des gleichen Passwortes dieser Update-Mechanismus umgangen werden. Für ein sicheres Netz müssen alle Accounts auf allen angeschlossenen Systemen ein schwer zu erratendes Passwort besitzen. Richtlinien sind hierzu oft:

  a. 6–8 Zeichen
  b. mindestens ein Sonderzeichen und eine Ziffer
  c. Update alle 3–6 Monate
  d. neues Passwort darf nicht eines der letzen 5 sein.

  Untersuchungen auf Systemen, die diese Richtlinien nicht einhalten, zeigen, daß etwa 10–20% der Passwörter leicht durch entsprechende Cracker-Tools geknackt werden können.
- Unnötige Dienste abschalten: Auf vielen Systemen laufen Server, die für den Betrieb dieses Rechners nicht benötigt werden. Oft werden diese defaultmäßig beim Systemstart mit gestartet. Dies ist nicht nötig und kann zu Sicherheitslücken führen, da diese dann meist auch nicht mit den neuesten Patches laufen (, da der Systemadministrator nicht daran denkt diese für diese Produkte einzuspielen).
- Nur die benötigten Zugriffsrechte vergeben: Viele Prozesse laufen aus Vereinfachung mit Prozeßrechten, die nicht für diese Aufgabe benötigt werden. Benutzer, die Privilegien haben, die sie für die spezielle Aufgabe nicht brauchen, können diese Privilegien mißbrauchen. Ferner können Prozesse durch Fehlprogrammierung anderen Prozessen Privilegien übertragen. Dies kann zu inheränten Sicherheitslücken führen.

Da leider die meisten Rechner am Netz Arbeitsplatzrechner sind und netzweit den Administratoren dieser Systeme nicht unbedingt allgemeingültige Vorschriften gemacht oder Sicherheits-Policies durchgesetzt werden können, scheint eine Sicherheitspolitik auf Rechner-Ebene allein nicht machbar. Ferner ist aufgrund der Zahl der angeschlossenen Systeme eine Kontrolle der einzelnen Rechner nicht durchführbar. Ein Ansatz auf Rechner-Basis kann nur zusätzliche Sicherheit erbringen. Eine zentrale Sicherheitsschranke, die für alle Systeme gleichzeitig wirkt, muß etabliert werden.

[4] Auch die eigene Passwort-Datei kann Rückschlüsse auf Passwörter auf anderen Rechnern geben. (Wer kommt nicht schnell aus Vereinfachungsgründen auf den Gedanken überall das gleiche Passwort zu benutzen.)

Betrachtet man die derzeitige Situation in der KFA, so scheint die Breite der möglichen Kommunikationspfade im ersten Moment aus Sicherheitsgesichtspunkten erschreckend.

- WiN-Anschluß,
- WiN-Testbed,
- EARN-Bitnet bzw. SNA Anschluß,
- allgemein X.25 Untervermittlung,
- ISDN-Anschluß zu WTI (mittelständisches Unternehmen in Jülich),
- Telephonzugang über Modems mit SLIP, PPP oder Terminal-Emulation,
- ISDN-Karten in PC's und
- wer weiß, vielleicht sogar Zugang über Funk.

Wie lassen sich alle diese Zugangsmöglichkeiten kontrollieren?

Betrachtet man die Situation etwas genauer, so entschärft sich die Lage doch erheblich. Zugänge über die allgemein verfügbaren Modems und über X.25 sind nur mit zusätzlichem Passwort möglich. Über die Modem-Leitungen ist ein Abhören nur mit krimineller Energie (Anzapfen des Telephons) möglich. Ähnliches gilt für die X.25 Leitung. Die Latenzzeiten der angeschlossenen Geräte lassen über Modem ein Ausspähen des Passwortes durch Probieren nur über sehr lange Zeitintervalle zu. Entsprechendes Logging sollte hier rechtzeitig Alarm schlagen.

Es verbleiben im Wesentlichen die externe WiN und WiN-Testbed Kommunikation, sowie der ISDN-Zugang zu der Firma WTI und die nicht bekannten Modem-Zugänge sowie weitere unbekannte Zugänge.

5 Allgemeine Design-Prinzipien und Philosophie

Die Implementierung eines Firewalls für die KFA setzt grundlegende Design-Prinzipien voraus, von denen bei der gesamten Installation nicht abgewichen werden sollte.

Security-Polices können im Wesentlichen in zwei Kategorien eingeteilt werden.

Was nicht grundsätzlich verboten ist, ist erlaubt.
Was nicht grundsätzlich erlaubt ist, ist verboten.

Läßt man alles zu, was nicht unsicher erscheint, so hält man ein sehr grosses potentielles Loch offen. Es werden Protokolle zugelassen, die vielleicht noch niemand bisher benutzt hat oder deren Sicherheitsmechanismen nicht richtig funktionieren, da sie nicht vollständig, in allen Einzelheiten, durchdacht oder erst garnicht implementiert wurden.

Der zweite Ansatz scheint für die Implementierung einer Security-Policy sinnvoller zu sein. Läßt man nur gewünschten Protokolle zu, so stellen Fehler in den anderen Protokollen kein Sicherheitsproblem dar. Sollte tatsächlich mal eine Sicherheitslücke entdeckt werden, so läßt sich diese schnell schließen. Werden weitere Protokolle gewünscht, so kann man diese leicht integrieren. Es muß nur ein weiteres Application-Gateway installiert; oder es müssen alternativ die Filter-Regeln im Router erweitert werden.

Software-Produkte können oft in verschiedene *Schubladen* einsortiert werden. Manche Programme gelten bekanntlich als gut, andere sind als unsicher bekannt. Problem-Programme sind meist komplex, enthalten mehrere tausend Zeilen Programm-Code und benötigen oft System-Privilegien. (Vergleiche hier die allgemeinen Aussagen zum Programm *sendmail*.) Um diese Problem-Programme zu adressieren, sollten die folgenden Basis-Design-Prinzipien berücksichtigt werden:

- Wenn jemals ein Fehler (Bug) in einem Software-Produkt auftreten sollte, so darf dieser nicht das Gesamtsystem kompromittieren.
- Rechner auf der ungeschützen Seite des Netzwerkes (außerhalb) sollten keine Netzwerk-Services ansprechen können, die mit Privilegien arbeiten.
- Netzwerk-Dienste sollten mit minimalen Features installiert werden und nur geringe Komplexität aufweisen. (Nur die Features zulassen, die auch gebraucht werden.) Der Quell-Code sollte klein und einfach genug sein. Er kann dann theoretisch gründlich und schnell überprüft werden.
- Es sollte eine Möglichkeit bestehen, die Korrektheit der Software mit überschaubarem Aufwand zu überprüfen.

Werden hohe Anforderungen an ein Firewall gestellt, so ist darauf zu achten, daß keine Hintertüren offengelassen werden (vergl. Modempool). Diese müssen mit allen zur Verfügung stehenden Mitteln geschlossen werden. Eine Security-Policy ist so schwach, wie das schwächste Glied in der Kette.

Sicherheits-Politik kann, wie die allgemeine Politik, nur betrieben werden, wenn alle am gleichen Strang ziehen. Sicherheit bedeutet praktisch immer Einschränkungen in der Funktionsweise oder aufwendigere Handhabung einer Funtion. Vieles ist möglich, aber manches muß unterbleiben. Unbekannte Zugänge, die sich aus dem Alltaggeschäft ergeben haben, müssen in die allgemeinen Pfade integriert, oder geschlossen werden. Sicherlich ist an der einen oder anderen Stelle eine Überwachung einer Versuchsanordnung über das Netz von außen notwendig. Dies kann aber immer über die allgemeinen Zugänge mit entsprechenden Sicherheitsvorkehrungen geschehen. Unbekannte Zugänge müssen per Dienstanweisung verboten werden, andernfalls dürfen die so erreichbaren Rechner nicht an KFAnet/Internet angeschlossen werden.

Als erster Schritt müssen die externen Zugänge, wie auch Modem-Zugänge, an einer Stelle gebündelt werden. Es entsteht so eine eindeutige wohldefinierte Schnittstelle zwischen internem und externem Netz. Das Glasfaser-Verbindungsnetz sei im folgenden mit KFA-secure-Net bezeichnet.

Ein Cisco Router, *zam301*, auf dem die neueste System-Software installiert (minimal 10.0), und der mit Access-Lists, Packet Filtern, konfiguriert ist, stellt bereits eine gute, wenn auch kleine, Hürde für externe Angreifer dar, wenn er als einziger Aufsatzpunkt für externen Datenverkehr in das Netz integriert wird.

Dieser Router erhält die folgenden Interfaces:

- FDDI zum externen Netz (ATM-Testbed), später generell externe Kommunikation
- FDDI zum internen Netz (KFAnet-FDDI-Backbone)
- X.25, derzeit noch für die externe Kommunikation zum WiN (Wissenschaftsnetz des DFN)
- Ethernet zu den Modem und ISDN Zugängen.

Modem-Zugänge, SLIP und PPP, sowie Zugänge über ISDN auf den Rechner *zam145* und der Zugang der Firma WTI über ISDN und den CISCO Router *zam200* werden in eigenen Subnetzen über ein gemeinsames Ethernet, also ein physikalisches Netz, gebündelt. Hierdurch können sämtliche Zugriffe mittels Abhören des Ethernet-Stranges kontrolliert und durch die Packet Screen *zam301*, falls erforderlich, abgeblocket werden.

Das derzeitige WiN-ATM-Testbed ist nur über einen weiteren WiN-DFN-Router, *zam300*, erreichbar. Hier können zusätzliche Packet Filter generiert werden.

Das KFA interne ATM Netz wird als dritte Komponente an den Glasfaser-Ring, *KFA-secure-Net*, über einen Cisco 7000, *zam002*, angeschlossen. Wiederum können durch Packet Filter Zugriffsmöglichkeiten erlaubt oder blockiert werden.

Durch die Konfiguration in unterschiedliche Teilnetze,

- ATM-Testbed
- ATM-KFA-intern
- KFAnet/INTERNET
- WiN-IP (X25)
- und externe Modem– und SLIP-Zugänge

können hier unterschiedliche Security-Policies definiert werden. Zugriff untereinander kann kontrolliert und gegebenfalls protokolliert werden.

Ein Firewall-Applikation-Gateway, *gatekeeper.kfa—juelich.de*, (im Folgenden kurz *gatekeeper*), kann für die Zugangskontrolle und für notwendige Applikationen oder Proxy-Server in das sogenannte *Screend Subnet*, *KFA-secure-Net*, integriert werden.

Dieses Gateway kann Applikationen wie Anonymous FTP, Netnews, WWW, Mail und Telnet aufnehmen. Eventuell werden hier nur sogenannte Proxy-Server installiert, wobei die wirklichen Server im internen Netz liegen können. In der ersten Planungsstufe ist das Application-Gateway nicht vorgesehen.

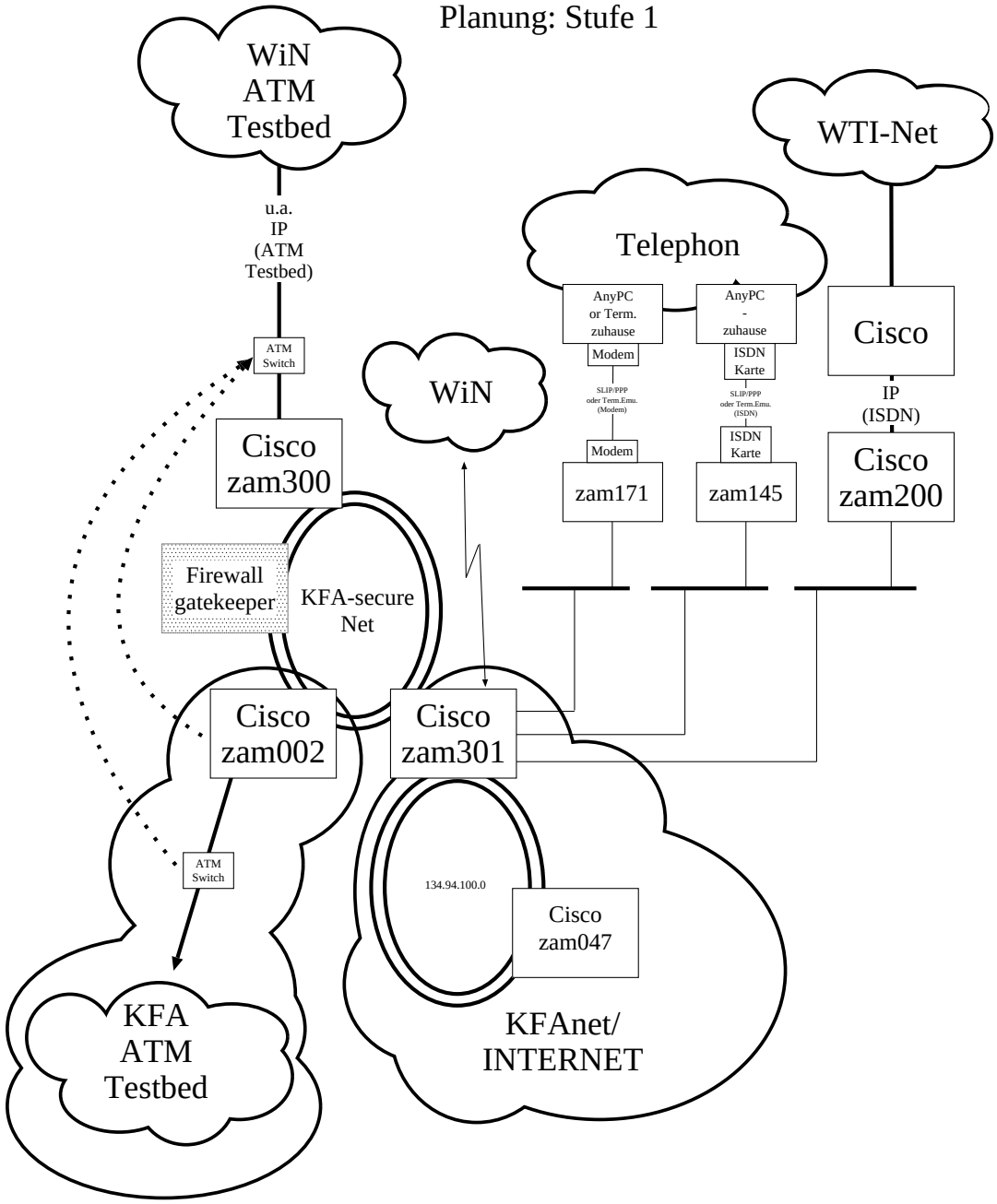


Abb. 15: Eine Lösung für die KFA auf kurze Sicht

7 Langfristige Lösungen

Wie bereits oben angedeutet sollte auf lange Sicht das Modem und ISDN Geschäft auf ein logisch und physikalisches Ethernet Segment zusammengefaßt und als solches behandelt werden.

Der Zugriff erfolgt nun transparent über das direkt am Ethernet angeschlossene Firewall-Applikation-Gateway. Dies stellt kein Security-Problem dar, da das Ethernet lokal installiert ist und direkter Zugriff (Abhören auf diesem) von extern nicht möglich ist. Passwörter schützen den unberechtigten Zugriff von außen. Nach Verifikation des Passwortes erfolgt die Durchschaltung der TCP/IP Verbindung (SLIP bzw. PPP Aufbau). Die Verbindung des WTI-Net ist durch interne Verdrahtung der ISDN-Adressen gegen Aufschaltung von außen geschützt. Die Mitarbeiter des WTI können aus Sicherheitsgesichtspunkten aufgrund eines Kooperationsvertrages als interne Mitarbeiter eingestuft werden. Das Innentätermodell wird allgemein in diesem Bericht nicht untersucht.

Der X.25 Zugang wird langfristig nicht mehr benötigt, da das ATM-Testbed in Produktion übergegangen ist. Backup des ATM 34 MBit Zuganges wird über X.25 am WiN-DFN-ATM Router realisiert. Für den Firewall stellt das keine Änderung dar.

Das Firewall-Applikation-Gateway, *gatekeeper*, wird installiert und mit den entsprechenden Applikationen bestückt.

An dieser Stelle steht die Überlegung an, welche Anwendungen von und nach extern zur Verfügung stehen müssen. Sicherlich sind aus Sicht der KFA die folgenden Dienste unabdingbar:

- E-Mail
- Netnews
- Telnet
- FTP
- WWW, XMosaic
- NQS bzw. NQE zu den Cray-Rechnern
- Archie zum Auffinden von Programmen und Dateien auf Anonymous FTP-Servern
- Whois für die Informationsgewinnung
- Finger für PGP-Schlüssel
- X-Protocol
- SNMP zu bestimmten Rechnern intern und eingeschränkt extern
- Domain Name Service
- ping,traceroute, nslookup, ...

Weitere Dienste können bei Bedarf und Notwendigkeit zusätzlich zugelassen werden.

Zur Vereinfachung lassen wir Verkehr zwischen internen Rechnern und unserem Gateway *gatekeeper* in beiden Richtungen zu. D.h. alle Services, die nicht benötigt werden, müssen auf diesem Rechner ausgeschaltet werden.

Die allgemeinen Default-Filter-Regeln, die Anwendung finden, wenn alle anderen nicht zutreffen sind dann:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	gatekeeper	*	134.94.0.0	*	ip	in	-
Allow	134.94.0.0	*	gatekeeper	*	ip	out	-
Deny	0.0.0.0	*	134.94.0.0	*	ip	in	-
Deny	134.94.0.0	*	0.0.0.0	*	ip	out	-

Tabelle 1 Default-Packet Filter

Hierbei ist unter Protokoll *ip* sowohl TCP, UDP als auch ICMP zu verstehen.

7.1 E-Mail

Mail-Zugang von aussen geschieht grundsätzlich über offizielle Mailadressen oder zumindest über MX-Records zum Mailrelay, *mailrelay.zam.kfa-juelich.de*. *Gatekeeper* kann mit niedrigerer Prioriät als secondary-mailrelay konfiguriert werden. Mail nach extern wird mittels *direct delivery* grundsätzlich sofort an den entfernten Rechner geleitet. Somit kann der TCP-Port 25 in der Packet Screen für eingehende Verbindungen für die meisten Rechner in der KFA gesperrt werden.

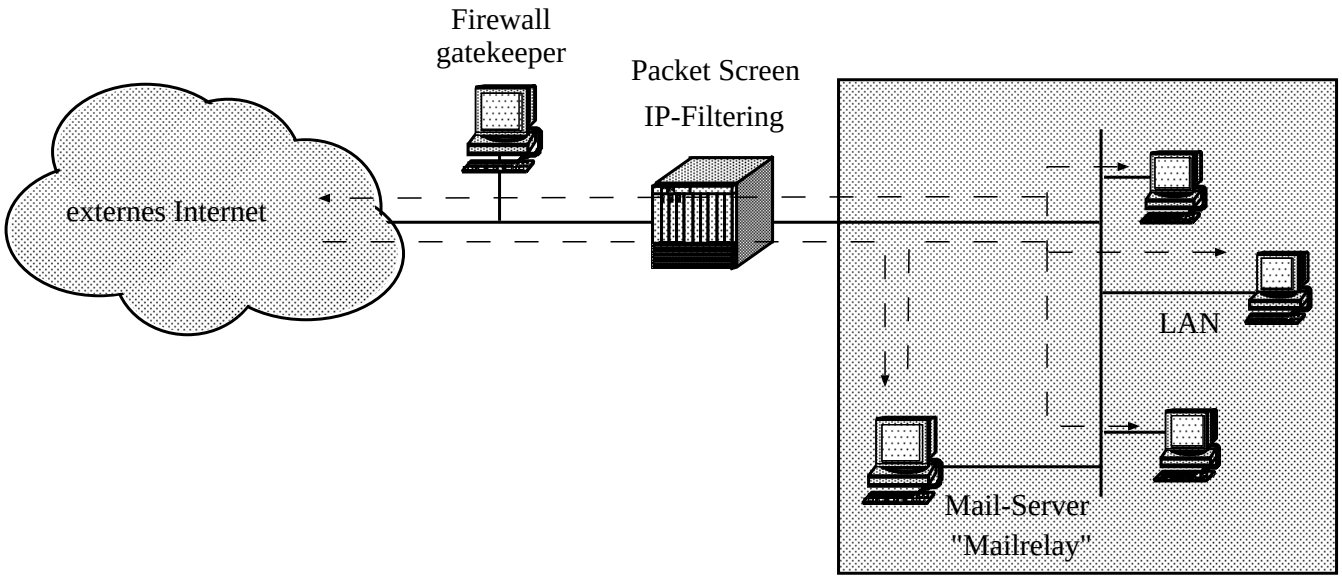


Abb. 16: mailrelay.zam.kfa-juelich.de

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Allow	0.0.0.0	*	mailrelay. KFA-Juelich.de	25	tcp	in	-
Allow	mailrelay. KFA-Juelich.de	25	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	0.0.0.0	25	tcp	out	-
Allow	0.0.0.0	25	134.94.0.0	*	tcp	in	establ.

Tabelle 2 Packet Filter für E-Mail

7.2 NetNews

Ähnlich ist die Situation für den Netnews Service konfigurierbar. Die externe Kommunikation bei Netnews beschränkt sich auf die beiden Rechner *netnews.zam.kfa-juelich.de* in der KFA und *sirius.dfn.de* beim DFN in Berlin. Diese beiden Rechner tauschen Artikel über den Port 119 aus. Source-Port ist jeweils ein unbekannter TCP-Port oberhalb 1024. Destination ist der TCP-Port 119. Client-Applikationen sprechen nur mit dem lokalen NetNews Server, führen also keine externe Kommunikation durch. Das folgende Bild zeigt den logischen Aufbau.

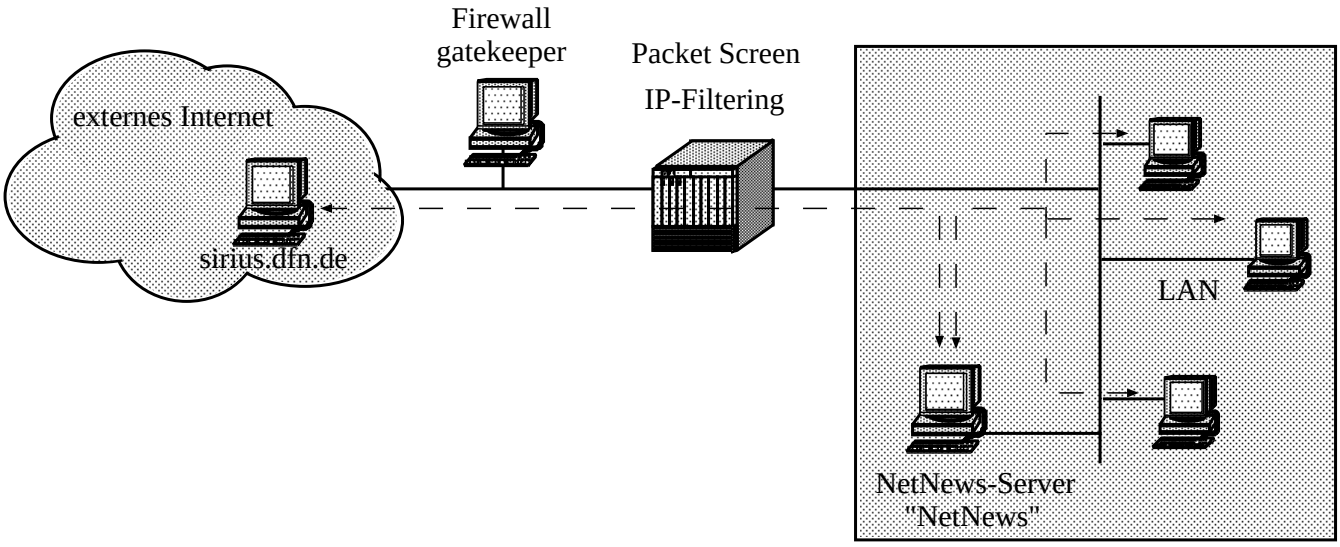


Abb. 17: netnews.zam.kfa-juelich.de

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	sirius.dfn.de	*	netnews. KFA-Juelich.de	119	tcp	in	-
Allow	netnews. kfa-juelich.de	119	sirius.dfn.de	*	tcp	out	establ.
Allow	netnews. KFA-Juelich.de	*	sirius.dfn.de	119	tcp	out	-
Allow	sirius.dfn.de	119	netnews. KFA-Juelich.de	*	tcp	in	establ.

Tabelle 3 Packet Filter für NetNews

7.3 Telnet

Das Telnet Protocol unterscheidet sich von den bisher betrachteten Anwendungen in einer ganz besonderen Weise. Um auf einen Account auf einem entfernten Rechner zugreifen zu können, muß der Benutzer ein geheimes Passwort eingeben. Dieses Passwort ist vielfältigen Attacken ausgesetzt. Meist wird zwar das eingegebene Passwort nicht am Terminal angezeigt (*echo off*), aber bei langsamer Eingabe kann ein geübter Zeitgenosse die Eingabefolge quasi *mitlesen*.

Ist das Passwort eingegeben worden, so geht es bei den meisten Telnet-Software-Lösungen unverschlüsselt über das Netz. Diejenigen, die Zugriff auf einen Teil der Netzwerk-Verbindung haben, z.B. einen Sniffer auf einem auf dem Weg liegenden Ethernet-Strang aufsetzen können, können UserId und Passwort mitlesen.

Der Cracker hat nun einen gültigen Account und ein dazu passendes Passwort. Die Attacke auf dem anzugreifenden System kann nun als Insider weitergehen. Root-Rechte sind nun noch leichter erreichbar.

Bei einer Telnet-Applikation kann man aus Sicht eines Firewalls zwei Fallunterscheidungen vornehmen.

- Der Benutzer will vom lokalen System aus auf einem entfernten Rechner arbeiten. Kompromittiert werden hier UserId und Passwort einer fremden Einrichtung. Diese Accounts zu schützen ist Aufgabe der fremden Organisation. Die Packet-Filter für diesen Fall auf einem Cisco-Router sind die folgenden:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.0.0	*	0.0.0.0	23	tcp	out	-
Allow	0.0.0.0	23	134.94.0.0	*	tcp	in	establ.

Tabelle 4 Packet Filter für Telnet von innen nach außen

- Der Benutzer will von einem entfernten System auf einem lokalen System arbeiten. Hier werden Accounts der eigenen Installation kompromittiert. Aus Sicht des einzelnen Benutzers mag dies nicht problematisch sein. *Wer will schon was mit meinen Daten anfangen?* Aus Sicht der Allgemeinheit stellt dies jedoch eine große Gefahr dar (vergleiche weiter oben *Net or Web of trust*). Dieser Fall erfordert eine gesonderte Behandlung. Für die Allgemeinheit am einfachsten zu implementieren, ist ein Telnet-Gateway. Benutzer, die von außen auf einen Rechner zugreifen wollen, müssen sich erst mit dem Gateway verbinden. Nach einer Authentisierung wird dann der Telnet-Verkehr transparent durch das Gateway durchgeschleust. Die Authentisierung erfolgt mittels:
  - Hand Held Authenticators, z.B. Security Dynamics — SecurID Cards [SecurID] oder Digital Pathways — SecureNet Key Cards
  - S/Key [Bellcore]
  - STEL [Vinzencetti,D.]
  - oder einem vergleichbaren Produkt.

Wichtig ist, daß die Authentisierung grundsätzlich durch ein Einmal-Passwort geschehen muß, damit nicht durch Abhören des Netzes gültige Passworte erspäht werden können. Wird die gesamte Session zusätzlich verschlüsselt, wie dies bei STEL der Fall ist, so kann dies der Sicherheit nur zuträglich sein. Günstig ist ein Telnet-Gateway, das mehrere oder alle Produkte unterstützt, da je nach Priorität und Sicherheitsbedürfnis Unterschiede gemacht werden können.

- Hand Held Authenticators — je Karte entstehen Kosten und Zusatzkosten für Software-Library. Die Verwendung eines einfachen (normalen) Telnet-Client ist möglich (Sicherheit: PIN + kartengeneriertem zeitabhängigem Access-Code → Einmalpasswort)
- S/Key — kostenlos erhältliche Software, Client und Server, (Sicherheit: Benutzer generiert einmalig Liste von Passwörtern, die er mit sich trägt, oder generiert jeweils das aktuelle Passwort aufgrund von nur ihm und dem Server bekannter Information → Einmalpasswort)
- STEL — Verschlüsselung der gesamten Session. Hier ist ein spezieller STEL-Client auf dem entfernten System notwendig. Ein Telnet-Gateway könnte entfallen, wenn auf allen lokalen Rechnern, zu denen von entfernter Stelle Zugriff erforderlich ist, STEL Server installiert werden. Es ist allerdings nicht zentral überprüfbar, ob dieser Server dann auch benutzt wird. STEL kann zusätzlich noch mit SecurID cards oder S/Key gesichert werden. (Sicherheit: Verschlüsselte Session inklusive UserId und Passwort)

Die Packet-Filter für diesen Fall sind:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	0.0.0.0	*	telnet-gate	23	tcp	in	-
Allow	telnet-gate	23	0.0.0.0	*	tcp	out	establ.

Tabelle 5 Packet Filter für Telnet von außen nach innen

Aus Sicht der KFA scheinen die Hand-Held Indicators nicht praktikabel. Die KFA stellt in ihrem Rechnerkontingent Rechenleistung für externe Benutzer in nicht zu vernachlässigender Menge zur Verfügung. Alleine auf den CRAY-Rechnern sind weit über 500 externe Benutzer eingetragen, die alle eine solche Karte benötigen würden. Hier treten enorme Kosten auf, die auch Folgeinvestitionen verursachen. Die am Markt erhältlichen Karten müssen alle drei Jahre erneuert werden, da die interne Batterie nicht länger hält.

Ferner ist bei einem solchen System der immense Personalaufwand zu berücksichtigen, der Ausgabe und Rücknahme der Karten, Verlustmeldungen, Fehlerbehebung etc. beinhaltet. Da gerade die CRAY-Rechner eine stark wechselnde Benutzerschaft aufweisen, wird hier der Personalaufwand noch zusätzlich erhöht.

Die Alternative S/Key stellt sich bei der Begutachtung als günstiger heraus. Auch hier muß jeder externe Benutzer in den Gateway-Rechner eingetragen und ein Anfangspasswort gesetzt werden. (Als externer Benutzer gilt auch ein Mitarbeiter, der sich temporär z.B. auf Dienstreise befindet.) Hier entfällt der Overhead der Kartenbestellung etc. Der

Benutzer muß seine Passwort-Liste in einer sicheren Umgebung selbst erstellen, ausdrucken und anschließend bei sich tragen. Dies ist allerdings schwierig für externe Benutzer, die nie lokal an einem KFA-Rechner arbeiten, sondern immer von entfernter Stelle aus über Telnet eingeloggt sind. Der Transfer einer Passwort-Liste über das Netz würde jedoch wieder ein Sicherheitsproblem darstellen.

Sinnvoll in der KFA-Umgebung ist sicherlich das STEL. Bei Eintragung eines Benutzers kann ein erstes Anfangspasswort eingetragen werden. Zukünftige Logins von entfernter Stelle werden immer verschlüsselt durchgeführt, demzufolge kann der Benutzer auch über das Netz hinweg sein Passwort sicher ändern. Häufiges Ändern des auf dem KFA-internen Rechner gespeicherten *Security-Keys* erhöht die Sicherheit der Session zusätzlich. Ein wesentlicher Vorteil des STEL in Verbindung mit einem TELNET-Gateway liegt darin, daß über die verschlüsselte Session zum Gateway hin nun KFA-interne UserId's und Passwörter für interne Telnet-Sessions übertragen werden können. (Diese sind nun, da sie Teil des Datastream der Telnet-Gateway Session sind, ebenfalls verschlüsselt.)

Ein allgemeiner Zugang über das Telnet Protokoll sollte nicht zur Verfügung gestellt werden, da die nichtverschlüsselte Übertragung eines Passwortes als Sicherheitsrisiko angesehen werden muß.

Das folgende Bild verdeutlicht den Datentransfer für Telnet-Verbindungen:

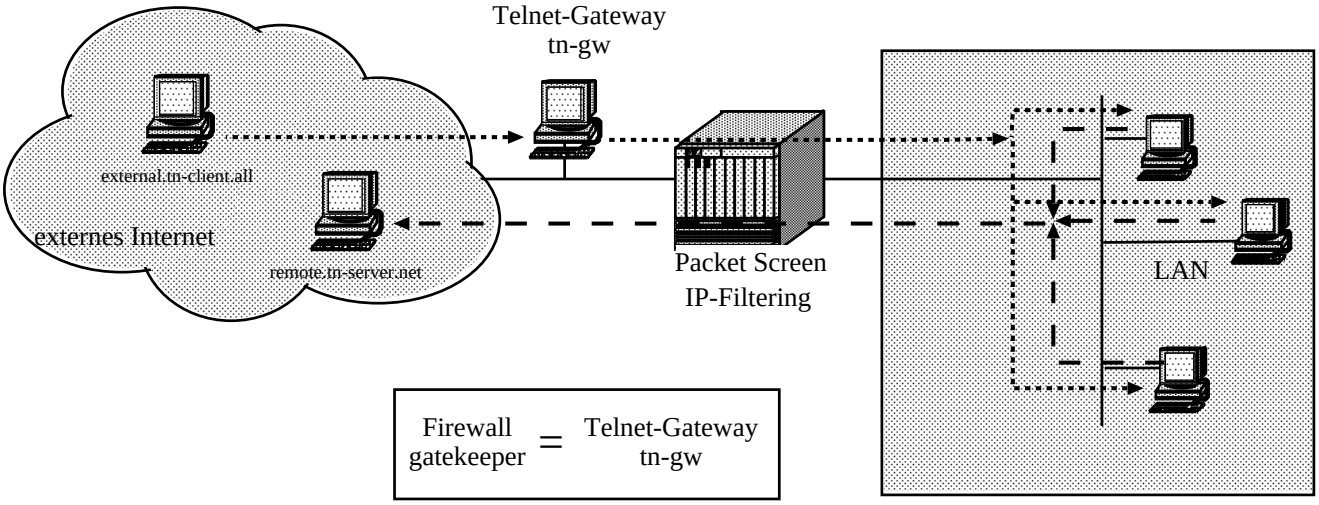


Abb. 18: tn-gw.zam.kfa-juelich.de

7.4 FTP

Protokolle, die es notwendig machen, daß der Server den Klienten zurückruft, sind sehr schwer durch ein Firewall managebar. Eines dieser Protokolle ist der Filetransfer. Beim FTP Protokoll wird durch den Benutzer eine sogenannte Kontroll-Verbindung aufgebaut (ähnlich einem Telnet-Kommando). Über diese Kontroll-Verbindung werden die Kommandos geschickt. Der tatsächliche Datentransfer (der Filetransfer) geschieht über eine zusätzliche Verbindung, die sogenannte Datenverbindung. Beim normalen FTP-Protokoll bedeutet dies, daß die Client-Software dem Server mitteilt auf welchem Port der Server den Clienten für den Datentransfer erreichen kann. Dieser baut dann eine Rückverbindung auf. Ein Firewall darf eine solche Verbindung nicht durchlassen, da es sich um eine Verbindung zu einem willkürklichen Port oberhalb der reservierten Ports handelt. Ob an diesem Port der Client oder ein zufälliger Server angesprochen wird, kann von der Firewall-Software nicht überprüft werden. Da die Kontroll- und Datenverbindung TCP/IP-mäßig unabhängig voneinander sind, kann also der Zusammenhang dieser beiden Sessions nicht nachvollzogen werden. Der Datentransfer muß blockiert werden.

Einen Ausweg aus diesem Dilemma würde das FTP-Subkommando *PASV* liefern. Dieses teilt dem Server mit, daß der Client die Datenverbindung aufbauen will. Somit besteht die FTP-Sitzung aus zwei von lokaler Seite initiierten TCP/IP-Verbindungen, die vom Firewall (in diesem Fall von der Packet-Screen) ohne Bedenken durchgelassen werden können. Leider steht das *PASV*-Sub-Kommando nicht in allen Server-Implementationen zur Verfügung.

Es erscheint hier sinnvoll alle diese Probleme zu umgehen, indem man Filetransfers nur von einem sicheren Rechner aus durchführt. Ein FTP-Gateway (FTP-Proxy-Server) bietet hier den besten Schutz.

Ein Benutzer im lokalen Netz, der eine FTP-Verbindung nach aussen initiieren will, verbindet sich mit dem FTP-Gateway-Server. Dieser *prompted* ihn nach dem entfernten Rechnernamen. Der FTP-Gateway-Server baut nun seinerseits eine FTP-Session zu dem entfernten Rechner auf und schaltet die FTP-Kommandos des internen Benutzers transparent durch. Die Packet Screen sieht nun nur noch FTP-Verbindungen zwischen internem Rechner und dem FTP-Gateway. Da das Gateway unter lokaler Kontrolle steht, kann sie TCP-Pakete in beiden Richtungen bedenkenlos durchlassen.

In gleicher Weise kann auch der FTP-Verkehr gehandhabt werden, der von externer Seite auf interne FTP-Server zugreift.

Bugs in der FTP-Server-Software, die von externen Hackern ausgenutzt werden könnten, werden so auf ein Minimum beschränkt. Der FTP-Proxy-Server steht den externen Benutzern an genau einer Stelle zur Verfügung. Werden Software-Bugs bekannt, so können sie zentral an dieser einen Stelle behoben werden. Notfalls, wenn kein Fix zur Verfügung steht, und es sich um einen ernst zu nehmenden Software-Fehler handelt, kann sogar der Server abgeschaltet werden. Ein Eindringen von Crackern ist dann nicht mehr möglich.

Anders all beim Telnet-Gateway wird hier die Zukunft zeigen, ob der FTP-Proxy das auf ihn zukommende Datenvolumen von mehreren parallelen FTP-Sessions verarbeiten kann und dabei nicht zum Bottleneck wird.

Nachteilig am FTP-Service ist derzeit noch, daß keine Verschlüsselung des Verkehrs möglich ist. UserId und Passwort gehen unverschlüsselt über das Netz. Ein z.B. SFTP, also ein äquivalentes Produkt zu STEL, ist derzeit nicht verfügbar. Es kann hier nur geraten werden auf File-Transfers zu lokalen UserId's zu verzichten und nur auf anonymous FTP-Server zuzugreifen, oder temporäre Accounts einzurichten, die nur für die Zeit des Datentransfers verfügbar sind.

Das folgende Bild verdeutlicht den Datentransfer für FTP-Verbindungen:

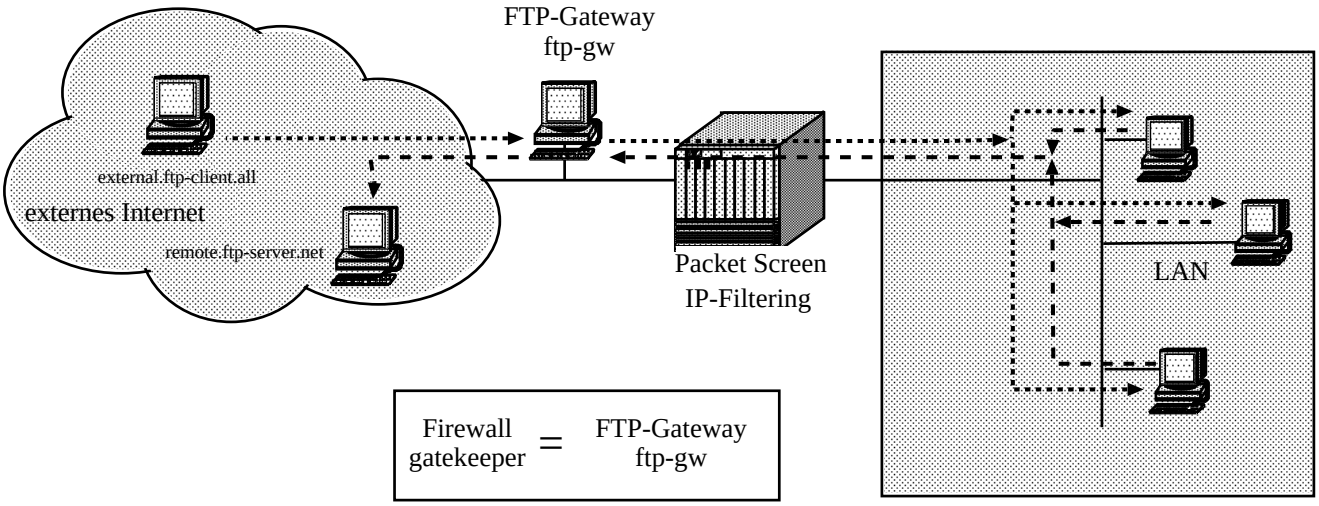


Abb. 19: ftp-gw.zam.kfa-juelich.de

7.5 WWW und Xmosaic

Die Internet “Killer” Applikation der 90iger Jahre ist sicherlich derzeit ohne Zweifel Mosaic und das WWW. Mittels WWW werden Gigabyte von Daten über die Netze geschickt. Obwohl dies aus Netzsicht gesehen nicht wünschenswert ist, sollte diese Applikation den Mitarbeitern der KFA nicht vorenthalten werden, da hierdurch auf einfachste Weise wertvolle Informationen weltweit verteilt und erhalten werden können.

Das World Wide Web (WWW, W3) ist das Universum von Netzwerk-zugreifbarer Information. Server bieten am Internet angeschlossenen Rechnern Daten an, die von Client-Maschinen gelesen werden können. Mit Proxy-Servern können Zugriffs-Kontrollmechanismen implementiert werden.

Betrachtet man das WWW aus Sicht einer Security-Policy so scheint es sehr schwer diese Mechanismen in ein Firewall Konzept zu integrieren.

Praktisch jeder Rechner in der KFA muß die Möglichkeit besitzen WWW-Server im Internet zu erreichen. Ein Proxy-Server, der als gemeinsame Schnittstelle für alle WWW-Requests fungiert, wird hier sehr schnell an seine Leistungsgrenzen gelangen. Es scheint also sinnvoll, WWW-Zugriffe nach extern von internen WWW-Zugriffen zu trennen.

Hierzu wird ein Proxy-WWW-Server extern installiert, der u.U. mit dem Firewall-Rechner identisch sein kann. Dieser Proxy-Server erhält WWW-Anfragen von internen Rechnern und leitet diese an externe WWW-Server weiter. Kommunikation der internen Maschinen mit externen nicht KFA-Rechnern ist somit nicht notwendig. Parallel dazu definiert man in der Client-Software die beiden internen WWW-Server als ***no-proxy***. D.h. Anfragen an interne WWW-Server werden direkt gestellt und nicht über den Proxy-Server vermittelt.

Sicherheitsbedenken ergeben sich vornehmlich bei der Ausführung von Scripts, die auf der lokalen Maschine, also intern in der KFA ausgeführt werden. Die NCSA Software stellt eine solche Schnittstelle zur Verfügung.

Vorsicht ist also auf der Anwender-Seite geboten. Scripts, die von einer wohlbekannten Site zur Verfügung gestellt werden, können wohl vorbehaltslos ausgeführt werden. Aber wo beginnen die *schwarzen Schafe*? Hier kann nur an den Benutzer appelliert werden, WWW nicht von einer privilegierten Task aus aufzurufen. Dies gilt auch für Informationen, die über WWW geladen und eventuell im Anschluß interpretiert werden. Dies gilt, z.B. für einen Postscript-File, der durch einen Postscript—Interpreter gelesen und anschließend angezeigt wird. Kontrollsequenzen innerhalb des Files können beliebige Kommandos auf dem Rechner auslösen. Eine Lösung dieser Probleme durch einen Proxy-Server ist nicht in Sicht. Es gibt genügend Angriffsmöglichkeiten. Hier kann nur der Rat gegeben werden, Vorsicht walten zu lassen.

Betrachtet man die andere Richtung, also Zugriff von aussen auf die internen WWW Server, so kann man die Sicherheitsprobleme wie folgt zusammenfassen.

Anfragen von externen Rechnern an die internen WWW-Server werden nur über den TCP-Port 80 zugelassen.

Angriffsziele sind vornehmlich unauthorisierter Zugriff auf Server-Daten und Nutzung des Servers für das Absetzen von System-Kommandos, also zusammengefaßt Ausnutzung von Bugs in der Serversoftware. Hier könnte ein Applikation-Gateway Zugriffsrechte

prüfen, verschiedene Zugriffsarten verbieten, Zugriff auf bestimmte Rechner beschränken, die Kommando-Sequenzen auf wohlgeformte Kommandos überprüfen usw..

Betrachtet man die derzeitige Situation in der KFA (2 installierte WWW-Server) so scheint jedoch ein eigener WWW-Proxy-Server für diesen Zweck zu aufwendig und nicht dringend notwendig zu sein. Die Sicherheit muß hier durch mehrere spezielle Merkmale so realisiert werden, daß keine Gefahr von einem eventuell kompromittierten Server ausgehen kann. Dies sind:

- Zugriff von aussen nur über TCP-Port 80 (insbesondere kein Telnet oder FTP von extern, etc.)
- immer die aktuell sicherste WWW-Software muß installiert sein, d.h. nicht unbedingt immer auch die neueste.
- Abschalten aller nicht unbedingt benötigten Server auf diesen Systemen

Hält man diese Regeln ein, so sollte von einem HTTP-Server (WWW-Server) keine große Gefahr ausgehen. Der WWW Service bzw. Mosaic kann dann den Mitarbeitern der KFA zur Verfügung gestellt werden. Ein ungutes Gefühl bleibt dennoch.

Die für die Implementation von WWW notwendigen Filter-Regeln lassen sich dann wie folgt zusammenfassen:

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Allow	0.0.0.0	*	www. KFA-Juelich.de	80	tcp	in	-
Allow	www. KFA-Juelich.de	80	0.0.0.0	*	tcp	out	establ.
Allow	0.0.0.0	*	www-upb. ipc.KFA-Juelich.de	80	tcp	in	*
Allow	www-upb. ipc.KFA-juelich.de	80	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	wwwproxy. kfa-juelich.de	80	tcp	out	-
Allow	wwwproxy. kfa-juelich.de	80	134.94.0.0	*	tcp	in	establ.

Tabelle 6 Packet Filter für WWW und Mosaic

Das logische Schaubild hierzu hat die folgende Form:

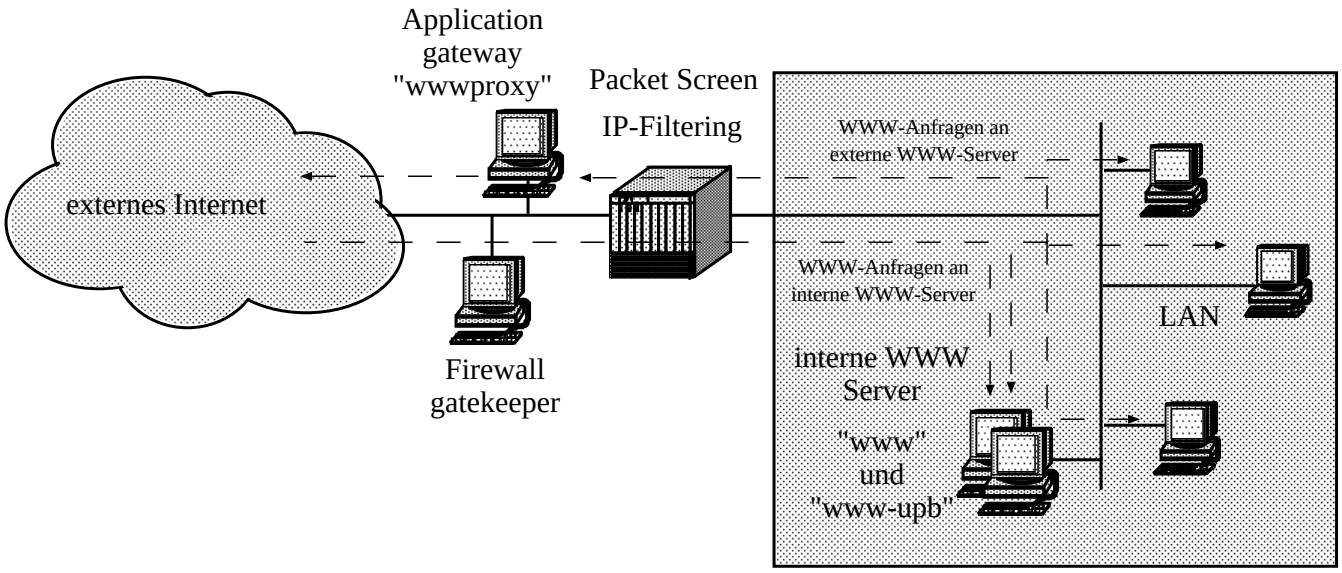


Abb. 20: WWW-(W3)-Service

7.6 NQS bzw. NQE zu den Cray-Rechnern

Die Firma Cray Research, Inc. bietet mit Network Queuing Environment (NQE) ein Software-Produkt an, das einem Benutzer den Versand, das Monitoring und die Kontrolle von Batch-Jobs erlaubt, die auf einem lokalen oder entfernten Rechner bearbeitet werden. Dieser Rechner nimmt die zu bearbeitenden Batch-Jobs mittels der Network Qeuing System Software (NQS) entgegen.

NQE stellt ein weiteres Software-Paket, Network Load Balancer (NLB), zur Verfügung, mit dem eine Ziel-Auswahl für die zu bearbeitenden Jobs durchgeführt und der Status der Batch Requests abgefragt werden kann.

Der File Transfer Agent (FTA) verwaltet (Queue-Verwaltung) die synchronen und asynchronen ein- und ausgehenden Datein, die über das Netz versandt werden.

Für ein funktionierendes NQS-System, bei dem die beiden Cray-Rechner als Server fungieren, ist also eine Kommunikation dieser beiden Systeme mit beliebigen Rechnern im Netz erforderlich.

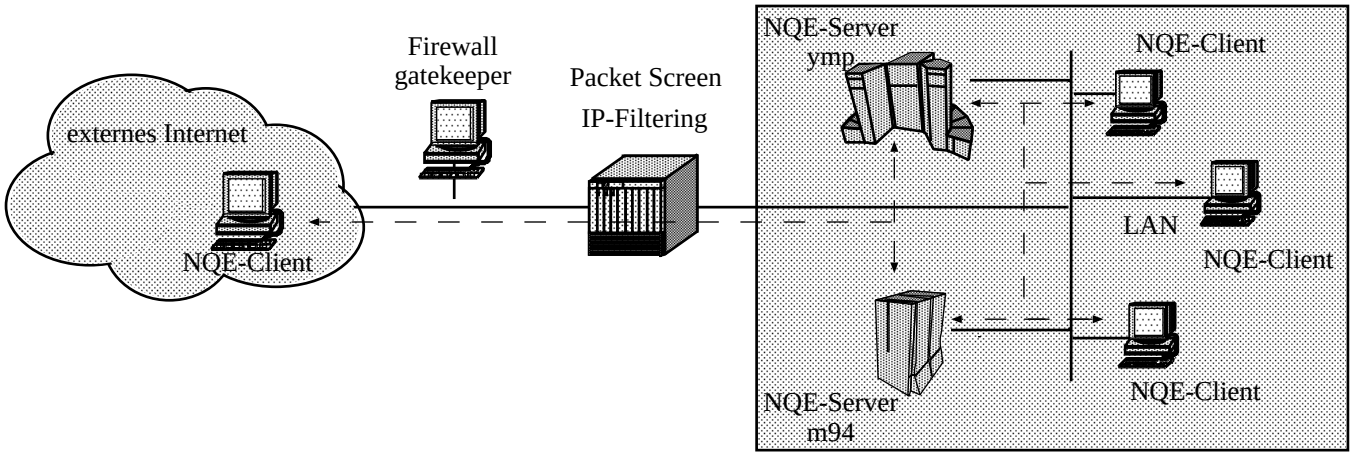


Abb. 21: NQS, NQE zu den Cray-Rechnern

Der Network Load Balancer (NLB) arbeitet über den TCP-Port 604, der File Transfer Agent (FTA) benutzt TCP-Port 605 und Network Queuing System (NQS) Requests werden über TCP-Port 607 verwaltet.

Hieraus ergibt sich für die zugehörigen Packet Filter:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	*	*	ymp.zam.KFA-Juelich.de	604	tcp	in	-
Allow	*	*	ymp.zam.KFA-Juelich.de	605	tcp	in	-
Allow	*	*	ymp.zam.KFA-Juelich.de	607	tcp	in	-
Allow	*	*	m94.zam.KFA-Juelich.de	604	tcp	in	-
Allow	*	*	m94.zam.KFA-Juelich.de	605	tcp	in	-
Allow	*	*	m94.zam.KFA-Juelich.de	607	tcp	in	-
Allow	ymp.zam.KFA-Juelich.de	604	*	*	tcp	out	establ.
Allow	ymp.zam.KFA-Juelich.de	605	*	*	tcp	out	establ.
Allow	ymp.zam.KFA-Juelich.de	607	*	*	tcp	out	establ.
Allow	m94.zam.KFA-Juelich.de	604	*	*	tcp	out	establ.
Allow	m94.zam.KFA-Juelich.de	605	*	*	tcp	out	establ.
Allow	m94.zam.KFA-Juelich.de	607	*	*	tcp	out	establ.

Tabelle 7 Packet Filter für NQS bzw. NQE

7.7 Archie

Das Archie Client-Programm wendet sich an eine allgemeine FTP Datenbank, um Informationen über einen vorgegebenen String zu erhalten. Im Allgemeinen handelt es sich hier um einen Dateinamen oder einen Suffix davon. Archie benutzt allgemein das Prospero Protokoll, das unter dem Port 191 (TCP/UDP) bzw. unter Port 1525 (UDP) läuft. Mittels des Archie Programmes lassen sich so auf einfache Weise anonymous FTP Server untersuchen, ob sie ein vorgegebenes Programm zur Verfügung stellen. Hierzu wird die externe FTP Datenbank täglich auf den neuesten Stand gebracht. Der Archie Service sollte den Mitarbeitern der KFA zur Verfügung stehen, um so schnellstmöglich und auf einfache Weise benötigte Programme zu erhalten.

Da die KFA selbst keinen Archie Server zur Verfügung stellt, handelt es sich hier aus der Sicht eines Firewalls um einen *einseitigen Dienst*. D.h. der Verbindungsaufbau geschieht grundsätzlich von der KFA aus.

Der Zugriff auf einen externen Archie-Server mittels UDP ist nicht zu empfehlen. Das Protokol an sich stellt keine großen Probleme dar, die Probleme entstehen allein durch die Benutzung von UDP. Da UDP ein verbindungsloses Protokoll ist, können Antworten eines Servers nicht eindeutig den entsprechenden Anfragen zugeordnet werden. Die eingehenden Pakete könnten sowohl Antworten auf Anfragen als auch Attacken gegen UDP basierte Dienste (NFS, Yellow Pages, ...) sein. D.h. es läßt sich nicht feststellen, ob es sich bei einer Verbindung von einem externen Host *hostx* mit Port 191 zu einem internen Rechner *hosty* Port z.b. 7193 um eine Antwort auf eine Archie Abfrage oder um ein eigenständiges Paket auf einen willkürlichen Port (Cracker-Aktivität) handelt. Solche Pakete lassen sich derzeit nur durch sogennate dynamische Paket-Filter erkennen, die aus einem verbindungslosen Protokoll, ein *quasi-verbindungsorientiertes* machen, indem sie Statusinformationen ausgehender UDP-Pakete speichern und diese mit eingehenden UDP-Paketen vergleichen.

In der KFA sollte daher das Anwendungsprogramm Archie bzw. Xarchie nicht zur Verfügung gestellt werden. Stattdessen kann man mittels Mosaic (HTTP-Protokoll) ebenfalls auf eine Reihe von Archie Servern zugreifen. Die Archie-Funktionalität steht hierdurch den Mitarbeitern der KFA zur Verfügung.

Ein geeigneter Aufsetzpunkt: für den Archie-Service mittels WWW ist z.B.

http://www.th-darmstadt.de/archie/archieplex.html

Von hieraus kann auch in eine Liste weiterer *Hypertext Archie Gateways* verzweigt werden. Die bekanntesten in dieser Liste sind:

ArchiePlexForm at NASA in den USA
— http://www.lerc.nasa.gov/Doc/archieplex-httpd.html

AA at NCSA in den USA
— http://hoohoo.ncsa.uiuc.edu/archie.html

ArchiePlexForm at NEXOR in UK (home of ArchiePlex)
— http://www.nexor.co.uk/archie.html

Im Allgemeinen sollte es jedoch reichen, den deutschen Server in Darmstadt zu kontaktieren.

7.8 Whois und Finger

Whois ist ein TCP transaktionsbasierender Dienst, der netzwerkweiten Directory-Dienst für Internet Benutzer zur Verfügung stellt [RFC-812]. U.a. werden Namen, Adressen und Telephon-Nummern, sowie Mailadressen von in der NIC (Network Information Center) Datenbank registrierten Personen gehalten. Inzwischen haben viele Institutionen (z.B. Ripe) Datenbanken angelegt, die über den Whois-Dienst abgefragt werden können. Die Whois-Client-Anwendung sollte demnach von intern nach extern über den Firewall zugelassen werden. In umgekehrter Richtung kann, wenn erforderlich, ein expliziter WHOIS-Server angelegt werden.

Entsprechendes gilt auch für den Finger-Dienst [RFC-1288]. Obwohl dieser aus Sicherheitsgründen (ausspionieren von Benutzern und Accounts) bisher nicht erwünscht war, kann er in einer sicheren Version nützliche Informationen über Benutzer zur Verfügung stellen. Gerade in der letzten Zeit wird er für die Verteilung öffentlicher Schlüssel für das PGP (Pretty Good Privacy) Protokoll verwendet. Einer Öffnung von intern nach extern ist nichts entgegenzusetzen, von extern nach intern sollte er nur auf einem zentral verwalteten Rechner verfügbar sein.

Aus diesen Überlegungen ergibt sich für die Packet Filter auf der Packet Screen:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zusatnd
Allow	134.94.0.0	*	0.0.0.0	43	tcp	out	-
Allow	0.0.0.0	43	134.94.0.0	*	tcp	in	establ.
Allow	0.0.0.0	*	whoisd. KFA-juelich.de	43	tcp	in	-
Allow	whoisd. KFA-Juelich.de	43	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	0.0.0.0	79	tcp	out	-
Allow	0.0.0.0	79	134.94.0.0	*	tcp	in	establ.
Allow	0.0.0.0	*	fingerd. KFA-Juelich.de	79	tcp	in	-
Allow	fingerd. KFA-Juelich.de	79	0.0.0.0	*	tcp	out	establ.

Tabelle 8 Packet Filter für Whois und Finger

Die folgende Graphik zeigt eine schematische Darstellung des Konzeptes. Whois- und Finger-Informationen werden gesammelt und auf einem (oder zwei) Server(n) abgelegt. Benutzer, die derartige Informationen verbreiten wollen, leiten diese an das Informationszentrum, das diese dann in den Server einspeist. Aufgrund der wohl vorerst nicht intensiven Nutzung dieses Dienste, können diese beiden zumindest vorläufig auch auf einem anderen Service–Rechner (z.B. NetNews-Server) installiert werden.

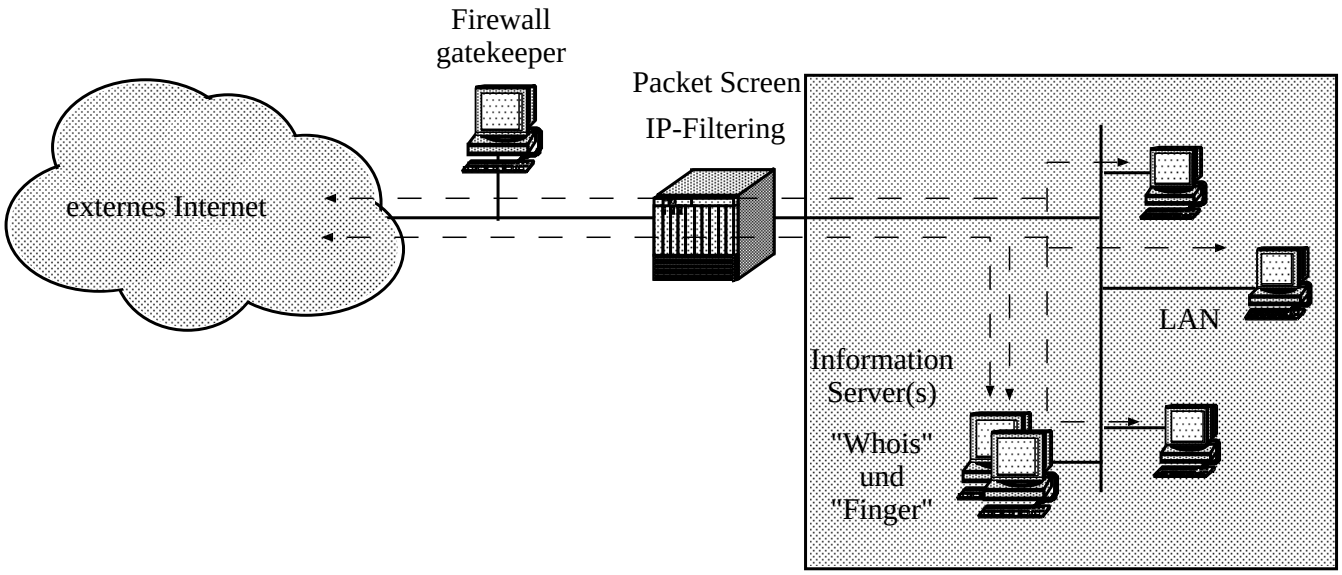


Abb. 22: Whois- und Finger Informations-Server

7.9 X-Protocol

Eine der kritischen Applikationen bei der Installation eines Firewalls ist das X Window System.

Das X-Window System ist eine Netzwerk-transparente graphische Benutzer-Interface Technologie für bitmapped Displays. Es ist eine Sammlung von Protokoll-Definitionen, File Formaten, Dokumentationen und einfachen Software Quell Programmen in C für Server, Klienten und Utility-Programme.

X unterscheidet sich von anderen graphischen Benutzerinterfaces, indem die graphische Funktionalität in einen Client- und Server-Teil aufgespalten wird. Der X-Server-Teil erhält exclusive Kontrolle über den Bildschirm und verteilt Anforderungen der Klienten.

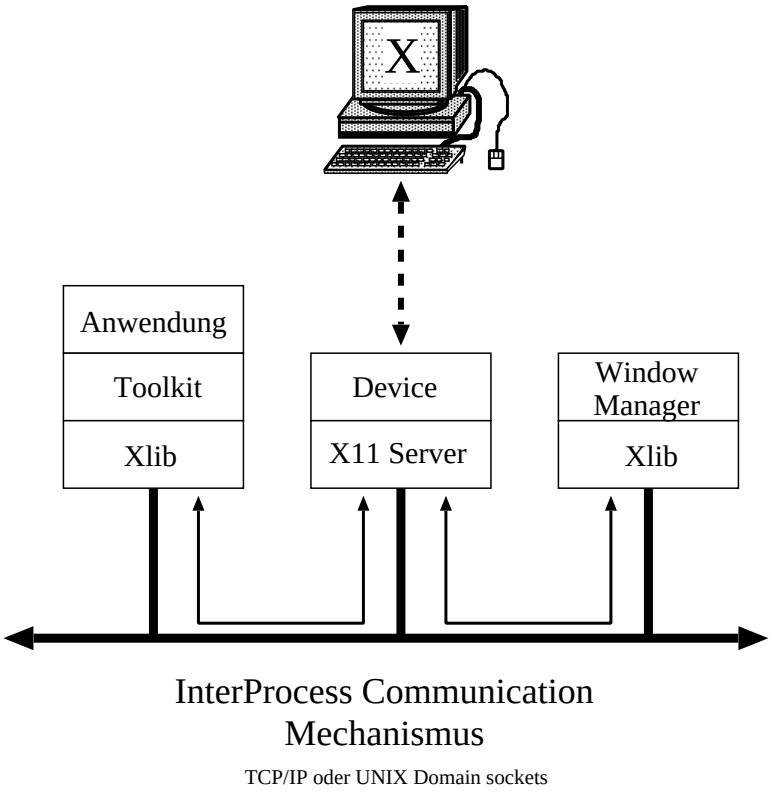


Abb. 23: X Window System Architektur

Da der X Server verschiedenen Client-Anwendungen Zugriff auf eine gemeinsame Ressource, den Bildschirm, erlaubt, ergibt sich ein potentieller Konflikt.

Server und Eingabe Aktivitäten werden den X-Anwendungen als Nachrichten, sogenannte *events*, übertragen. Wenn ein Window für eine Anwendung eröffnet wird, wird in eine Liste eingetragen, über welche events diese Anwendung unterrichtet werden soll. Steht Eingabe oder Server-Aktivität an, überprüft der Server, an welche X-Anwendungen diese geleitet werden sollen. Obwohl normalerweise ein Client nur über *events* im eigenen Window informiert wird, kann er verlangen, über alle *events* informiert zu werden. Dies bedeutet, daß er alle Eingaben, also auch *login requests* und Passwörter mitlesen kann. Dies bedeutet ein großes Sicherheitsrisiko.

Das Basis Sicherheitsmodell für X Windows erlaubt dem Benutzer, die Menge der Rechner zu bestimmen, die Verbindungen zu seinem X Server aufnehmen dürfen.

Forscher kollaborieren oft mit Forschern anderer Forschungseinrichtungen und Universitäten unter Benutzung des X Window Systems.

Da die Sicherheitsmechanismen nicht Benutzerbezogen sind, bleibt nur ein Rechner basierter Ansatz. Dies führt allerdings zum Problem, daß andere Benutzer auf dem berechtigten entfernten System ebenfalls Zugriff auf dem lokalen System erhalten können. Dieser Ansatz muß als falsch angesehen werden.

Eine weitere Möglichkeit stellt XAuthority dar. Hier wird in der Datei .Xauthority ein sogenanntes *MIT-MAGIC-COOKIE* eingetragen. Nur Client-Applikationen, die dieses Magic-Cookie kennen, erhalten Zugriff auf den X-Server dieses Rechners. So gesehen stellt dieses *Magic-Cookie* ein benutzerbezogenes Sicherheitssystem dar. Für einen Einsatz im externen Bereich ist es allerdings nicht einsetzbar, da das *Magic-Cookie* unverschlüsselt übertragen wird. Ein Cracker, der dieses liest, kann dann unberechtigten Zugriff auf den X-Server dieses Rechners erhalten und obige Sicherheitslücken ausnutzen.

Einen Lösungsansatz bietet das xforward Programm [Treese,G.W., Wolman,A.] Hier wird ein Gateway Rechner installiert, auf dem ein Benutzer in einer *restricted shell* das Kommando

xforward –display *lokaler_Rechner* **–allow** *entfernter_Rechner*

absetzt. xforward gibt eine Port-Nummer zurück an die er sich vom entfernten Rechner aus mit seiner Applikation wenden kann. Die Ein- und Ausgaben werden dann zwischen *lokaler_Rechner* und *entfernter_Rechner* über das Gateway geleitet. Dies alles würde noch keine Sicherheitsverbesserung erbringen. Knack-Punkt ist nun, daß bevor die Durchleitung geschaltet wird, das Gateway ein POPUP-Fenster auf dem lokalen Rechner öffnet, indem der lokale Benutzer bestätigen muß, das diese Verbindung, also genau diese eine X-Anwendung, zulässig ist. Somit hat der Benutzer wieder absolute Kontrolle über sein Display.

Direkte X-Verbindungen zwischen lokalem Rechner und entferntem Rechner brauchen nicht auf der Packet Screen durchgelassen zu werden.

Das an dieser Stelle zu dem *xforward*-Programm gesagte, gilt in gleicher Weise auch für das Programm *x-gw* im sogenannten Firewall-Toolkit der Firma Trusted Information Systems (TIS).

Die notwendigen Filter-Regeln sind die folgenden (Es sei hier angenommen, daß der Zugriff auf die *restricted shell* über Port 5999 geschieht. Das X-Windows-Protokoll kommuniziert über die Ports 6000 – 6999):

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zusatnd
Deny	0.0.0.0	*	Xwingate. KFA-Juelich.de	>6999	tcp	in	-
Allow	0.0.0.0	*	Xwingate. KFA-Juelich.de	>5998	tcp	in	-
Deny	Xwingate. KFA-Juelich.de	>6999	0.0.0.0	*	tcp	out	-
Allow	Xwingate. KFA-Juelich.de	>5998	0.0.0.0	*	tcp	out	-

Tabelle 9 Packet Filter für X-Window-System

Wird das xforward-Programm auf dem Firewall-Rechner *gatekeeper* selbst installiert (*gatekeeper=Xwingate*), so sind keine Filter-Regeln erforderlich, da die Kommunikation zwischen dem Firewall gatekeeper und internen Rechnern aufgrund der Default-Regeln erlaubt ist.

7.10 SNMP

Das Simple Network Management Protocol (SNMP) wird benutzt, um Rechner innerhalb der Internet-Community zu verwalten. Langfristig soll SNMP durch das OSI Network Management abgelöst werden. SNMP kommuniziert über die UDP Ports 161 und 162.

Allgemein kann an dieser Stelle gesagt werden, daß ausschließlich das KFAnet/Internet Management die Notwendigkeit hat, SNMP Requests nach außen abzusetzen. Aus Vereinfachungsgründen kann dies von einem Rechner aus geschehen.

Rechner innerhalb der KFA müssen nicht von extern administriert werden. SNMP-Zugang von extern wird daher nicht erlaubt.

Die einzigen Rechner, die ein externes Management, bzw. eine externe Überwachung erfordern sind die ans internationale Netz angeschlossenen Cisco-Router. Diese sind aber vor der Packet Screen gelegen, brauchen also in dieser nicht extra berücksichtigt zu werden.

Die Filter-Regeln für SNMP können somit wie folgt spezifiziert werden:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zusatnd
Allow	zam244.zam. KFA-Juelich.de	*	0.0.0.0	161	udp	out	-
Allow	zam244.zam. KFA-Juelich.de	*	0.0.0.0	162	udp	out	-
Allow	0.0.0.0	161	zam244.zam. KFA-Juelich.de	*	udp	in	-
Allow	0.0.0.0	162	zam244.zam. KFA-Juelich.de	*	udp	in	-

Tabelle 10 Packet Filter für SNMP

7.11 Domain Name Service

Grundlage fast jeder TCP/IP Kommunikation ist die Auflösung vonRechnernamen auf Rechneraddressen. Dieser Dienst wird von einem sogenannten Nameserver zur Verfügung gestellt.

Der DNS Dienst benötigt sowohl den TCP Port 53 als auch den UDP Port 53 . Der UDP Port 53 wird im allgemeinen für Client-zu-Server Anfragen (wobei die Client Seite einen zufälligen Port benutzt) und für Proxy Server-zu-Server Anfragen (wobei ein Server einen anderen in Vertretung für einen Clienten fragt) benutzt. Der TCP-Dienst wird allgemein für einen Server-zu-Server Bulk Transfer benutzt (typischerweise für Zonen Transfers zwischen Primary und Secondary Server).

Die meisten DNS Server Implementationen (z.B. BIND) benutzen für die Server-zu-Server Kommunikation auf beiden Seiten den UDP Port 53. Diese Eigenschaft kann für Packet Filtering gut genutzt werden. Es kann hier ausschließlich Verkehr auf UDP Port 53 zwischen Source und Destination zugelassen werden. Jeder andere UDP-Verkehr hat zu unterbleiben, um ein Vortäuschen des Nameservers zu verhindern. (Sonst könnte ein externer Rechner einem Client falsche Antworten des Nameservers unterjubeln.)

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.80.2	53	0.0.0.0	*	udp	out	-
Allow	134.94.80.2	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.80.2	53	udp	in	-
Allow	ns.nic.de	53	134.94.80.2	53	tcp	in	-

Tabelle 11 Packet Filter für DNS (*Primary Nameserver*)

Die gleichen Zugriffs-Filter müssen auch für den *Secondary Nameserver* generiert werden.

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.80.3	53	0.0.0.0	*	udp	out	-
Allow	134.94.80.3	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.80.3	53	udp	in	-
Allow	ns.nic.de	53	134.94.80.3	53	tcp	in	-

Tabelle 12 Packet Filter für DNS (*Secondary Nameserver*)

Eine zusätzliche Besonderheit in der KFA stellt die Subdomain *sp* dar. Für diese Subdomain ist der Rechner *zam226–e01.zam.kfa-juelich.de* zuständig. Demzufolge muß dieser ebenfalls in die Packetfilter mit einbezogen werden.

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.100.24	53	0.0.0.0	*	udp	out	-
Allow	134.94.100.24	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.100.24	53	udp	in	-
Allow	ns.nic.de	53	134.94.100.24	53	tcp	in	-

Tabelle 13 Packet Filter für DNS, Subdomain *sp*(*Nameserver für IBM/SP2*)

Entsprechendes gilt für den Backup-Fall, wenn das *134.94.100.24*–iger Interface nicht zur Verfügung steht. Die Packetfilter lauten hier:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.100.25	53	0.0.0.0	*	udp	out	-
Allow	134.94.100.25	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.100.25	53	udp	in	-
Allow	ns.nic.de	53	134.94.100.25	53	tcp	in	-

Tabelle 14 Packet Filter für DNS, Subdomain *sp*, Backup (*Nameserver für IBM/SP2*)

Zonentransfers der Domain *kfa-juelich.de* über das TCP-Protokoll werden grundsätzlich nicht erlaubt. Eine Ausnahme stellt der Transfer zum Rechner *ns.nic.de* dar (Externer Backup Nameserver).

Zusätzliche Einträge müssen für den Secondary Nameserver des DE-NIC gemacht werden. Sollten die Nameserver der KFA einmal nicht antworten, so fragt ein Client den DE-NIC Nameserver nach den aufzulösenden Namen. Diese Kommunikation muß erlaubt sein und entsprechende Filter-Regeln müssen generiert werden.

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	134.94.0.0	*	ns.nic.de	53	udp	out	-
Allow	ns.nic.de	53	134.94.0.0	*	udp	in	-

Tabelle 15 Packet Filter für DNS Anfragen zu *ns.nic.de* als Backup Server

7.12 Ping, Traceroute, Nslookup et all

ICMP stellt nach allgemeiner Meinung kein Sicherheitsproblem dar.

Das Ping Programm, das Erreichbarkeitsinformationen liefert, sollte auch von einem durch Firewall geschützen Netz aus ausführbar sein. Ping ist ein auf dem ICMP Protokoll basierendes Programm. Das Ping Programm setzt ein Echo-Request-Paket ab und erwartet als Antwort ein Echo-Reply-Paket. Da ICMP nicht beschränkt wird, kann ein *ping*-Request auch zu externen Rechnern hin durchgeführt werden. Die Antwort-Pakete gelangen ungehindert an den Absender zurück.

Bei Traceroute haben wir es mit einer anderen Situation zu tun. Traceroute setzt ein UDP-Paket an einen nicht benutzen, fiktiven Port ab. Erwartet wird als Antwort eine Port-Unreachable-ICMP-Message. Erlauben wir UDP-Pakete von intern nach extern, so ist auch hier eine Kommunikation gewährleistet, da ja die Antwort-Pakete zugelassen werden (ICMP).

Ein besonderes Problem stellt Nslookup dar. Hier wird von einem beliebigen UDP-Port intern mit dem speziellen UDP-Port 53 extern kommuniziert. Antwort-Pakete kommen also von UDP-Port 53 auf einen vorher vereinbarten zufälligen UDP-Port. Dies kann aus Sicherheitsgründen nicht zugelassen werden, da nicht nachprüfbar ist, welcher Prozess sich hinter dem externen UDP-Port 53 verbirgt, und UDP keine Relation zwischen den beiden Kommunikationsrichtungen herstellt. Es gibt z.B. kein Acknowledgement oder Synchronize-Paket. Die beiden Kommunikationrichtungen sind unabhängig voneinander.

An dieser Stelle wird empfohlen das Programm Nslookup in eingeschränkter Form zur Verfügung zu stellen. Defaultmäßig wird bei Nslookup der lokale Server kontaktiert. Erst durch Absetzen des Subkommandos **set server=*servername*** entsteht eine Kommunikationsverbindung und somit ein Kommunikationsstrom vom Benutzer-Rechner zu einem externen Nameserver. Wird diese Funktion dem normalen Benutzer nicht zur Verfügung gestellt, so kommt man ohne ein zusätzliches Gateway für Nslookup aus.

Die für diese Kommunikationen notwendigen Filterregeln sind die folgenden:

Zugriff	Source IP	Source Port	Destination IP	Destination Port	Protocol	Richtung	Zustand
Allow	0.0.0.0	*	0.0.0.0	*	icmp	in	-
Allow	0.0.0.0	*	0.0.0.0	*	icmp	out	-
Allow	134.94.0.0	*	0.0.0.0	*	udp	out	-

Tabelle 16 Packet Filter für *ping*, *traceroute* und *nslookup*

7.13 Die Filter-Regeln für die KFA relevanten Services

Im folgenden sind nun die für die KFA relevanten Filter-Regeln in einer Gesamt-Tabelle zusammengefaßt. Es muß auf die Reihenfolge der Filter-Regeln geachtet werden, da sonst Lücken im Firewall Konzept auftreten können.

Die Filter-Regeln berücksichtigen, daß auf dem Firewall-Rechner gatekeeper die Services Telnet-Gateway, FTP-Gateway, HTTP-Gateway und X-Gateway laufen. Diese brauchen also auf dem zum internen Netz hin liegenden Router nicht berücksichtigt zu werden.

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Packet Filter für E-Mail							
Allow	0.0.0.0	*	mailrelay. KFA-Juelich.de	25	tcp	in	-
Allow	mailrelay. KFA-Juelich.de	25	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	0.0.0.0	25	tcp	out	-
Allow	0.0.0.0	25	134.94.0.0	*	tcp	in	establ.
Packet Filter für NetNews							
Allow	sirius.dfn.de	*	netnews. KFA-Juelich.de	119	tcp	in	-
Allow	netnews. kfa-juelich.de	119	sirius.dfn.de	*	tcp	out	establ.
Allow	netnews. KFA-Juelich.de	*	sirius.dfn.de	119	tcp	out	-
Allow	sirius.dfn.de	119	netnews. KFA-Juelich.de	*	tcp	in	establ.
Packet Filter für Telnet-Gateway (entfallen, da gatekeeper=tn-gw)							
Packet Filter für Telnet nach extern							
Allow	134.94.0.0	*	0.0.0.0	23	tcp	out	-
Allow	0.0.0.0	23	134.94.0.0	*	tcp	in	establ.
Packet Filter für Whois (Port 43) und Finger (Port 79)							
Allow	134.94.0.0	*	0.0.0.0	43	tcp	out	-
Allow	0.0.0.0	43	134.94.0.0	*	tcp	in	establ.
Allow	0.0.0.0	*	whoisd. KFA-juelich.de	43	tcp	in	-
Allow	whoisd. KFA-Juelich.de	43	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	0.0.0.0	79	tcp	out	-
Allow	0.0.0.0	79	134.94.0.0	*	tcp	in	establ.
Allow	0.0.0.0	*	fingerd. KFA-Juelich.de	79	tcp	in	-
Allow	fingerd. KFA-Juelich.de	79	0.0.0.0	*	tcp	out	establ.

Tabelle 17 Zusammenfassung der Packet Filter

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Packet Filter für X-Window-System (entfallen da *gatekeeper=Xwingate*)							
Packet Filter für SNMP							
Allow	zam244.zam. KFA-Juelich.de	*	0.0.0.0	161 162	udp	out	-
Allow	0.0.0.0	161 162	zam244.zam. KFA-Juelich.de	*	udp	in	establ.
Packet Filter für allgemeine DNS Anfragen zu *ns.nic.de*							
Allow	134.94.0.0	*	ns.nic.de	53	udp	out	-
Allow	ns.nic.de	53	134.94.0.0	*	udp	in	-
Packet Filter für DNS (*Primary Nameserver*)							
Allow	134.94.80.2	53	0.0.0.0	*	udp	out	-
Allow	134.94.80.2	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.80.2	53	udp	in	-
Allow	ns.nic.de	53	134.94.80.2	53	tcp	in	-
Packet Filter für DNS (*Secondary Nameserver*)							
Allow	134.94.80.3	53	0.0.0.0	*	udp	out	-
Allow	134.94.80.3	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.80.3	53	udp	in	-
Allow	ns.nic.de	53	134.94.80.3	53	tcp	in	-
Packet Filter für DNS, Subdomain sp (*Primary Nameserver*)							
Allow	134.94.100.24	53	0.0.0.0	*	udp	out	-
Allow	134.94.100.24	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.100.24	53	udp	in	-
Allow	ns.nic.de	*	134.94.100.24	53	tcp	in	-
Packet Filter für DNS, Subdomain sp (*Secondary Nameserver*)							
Allow	134.94.100.25	53	0.0.0.0	*	udp	out	-
Allow	134.94.100.25	53	0.0.0.0	*	tcp	out	-
Allow	0.0.0.0	*	134.94.100.25	53	udp	in	-
Allow	ns.nic.de	*	134.94.100.25	53	tcp	in	-
Packet Filter für *ping*							
Allow	0.0.0.0	*	0.0.0.0	*	icmp	in	-
Allow	0.0.0.0	*	0.0.0.0	*	icmp	out	-
Packet Filter für *traceroute*							
Allow	134.94.0.0	*	0.0.0.0	*	udp	out	-

Tabelle 18 Zusammenfassung der Packet Filter (continued)

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Packet Filter für WWW und Mosaic							
Allow	0.0.0.0	*	www. KFA-Juelich.de	80	tcp	in	-
Allow	www. KFA-Juelich.de	80	0.0.0.0	*	tcp	out	establ.
Allow	0.0.0.0	*	www-upb. ipc.KFA-Juelich.de	80	tcp	in	*
Allow	www-upb. ipc.KFA-juelich.de	80	0.0.0.0	*	tcp	out	establ.
Allow	134.94.0.0	*	wwwproxy. kfa-juelich.de	80	tcp	out	-
Allow	wwwproxy. kfa-juelich.de	80	134.94.0.0	*	tcp	in	establ.
Packet Filter für NQS bzw. NQE							
Allow	*	*	ymp.zam.KFA- Juelich.de	604 605 607	tcp	in	-
Allow	*	*	m94.zam.KFA- Juelich.de	604 605 607	tcp	in	-
Allow	ymp.zam.KFA- Juelich.de	604 605 607	*	*	tcp	out	establ.
Allow	m94.zam.KFA- Juelich.de	604 605 607	*	*	tcp	out	establ.
Default-Packet-Filter							
Allow	gatekeeper	*	134.94.0.0	*	ip	in	-
Allow	134.94.0.0	*	gatekeeper	*	ip	out	-
Allow	0.0.0.0	*	134.94.0.0	*	icmp	in	-
Allow	134.94.0.0	*	0.0.0.0	*	icmp	out	-
Deny	0.0.0.0	*	134.94.0.0	*	ip	in	-
Deny	134.94.0.0	*	0.0.0.0	*	ip	out	-

Abb. 24: Zusammenfassung der Packet Filter (continued 2)

Die folgende Tabelle berücksichtigt zusätzlich, daß ausgehende Pakete keinen Schaden anrichten können, wenn der rückwärtige Verkehr verboten ist. Die obigen Regeln lassen sich also noch stark vereinfachen und zusammenfassen. Die resultierenden Filterregeln sind die folgenden:

Zugriff	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Richtung	Zustand
Allow	0.0.0.0	23 25 43	134.94.0.0	*	tcp	in	establ.
Allow	ns.nic.de	53	134.94.80.2 134.94.80.3 134.94.100.24 134.94.100.25	53	tcp	in	-
Allow	0.0.0.0	79	134.94.0.0	*	tcp	in	establ.
Allow	sirius.dfn.de	119	netnews.KFA-Juelich.de	*	tcp	in	establ.
Allow	0.0.0.0	*	mailrelay.KFA-Juelich.de	25	tcp	in	-
Allow	0.0.0.0	*	whoisd.KFA-juelich.de	43	tcp	in	-
Allow	0.0.0.0	*	fingerd.KFA-Juelich.de	79	tcp	in	-
Allow	0.0.0.0	*	www.KFA-Juelich.de	80	tcp	in	-
Allow	0.0.0.0	*	www-upb.ipc.KFA-Juelich.de	80	tcp	in	-
Allow	sirius.dfn.de	*	netnews.KFA-Juelich.de	119	tcp	in	-
Allow	0.0.0.0	*	ymp.zam.KFA-Juelich.de m94.zam.KFA-Juelich.de	604 605 607	tcp	in	-
Allow	0.0.0.0	161 162	zam244.zam.KFA-Juelich.de	*	udp	in	-
Allow	ns.nic.de	53	134.94.0.0	*	udp	in	-
Allow	0.0.0.0	*	134.94.80.2 134.94.80.3 134.94.100.24 134.94.100.25	53	udp	in	-
Allow	0.0.0.0	*	134.94.0.0	*	icmp	in	-
Allow	gatekeeper	*	134.94..0.0	*	ip	in	-
Allow	134.94.0.0	*	0.0.0.0	*	ip	out	-
Deny	0.0.0.0	*	134.94.0.0	*	ip	in	-

Ein schematisches Firewall-Netz-Layout zeigt die folgende Graphik. Nicht alle dargestellten Server müssen auf unterschiedlichen Systemen zur Verfügung gestellt werden.

Schematische Sicht

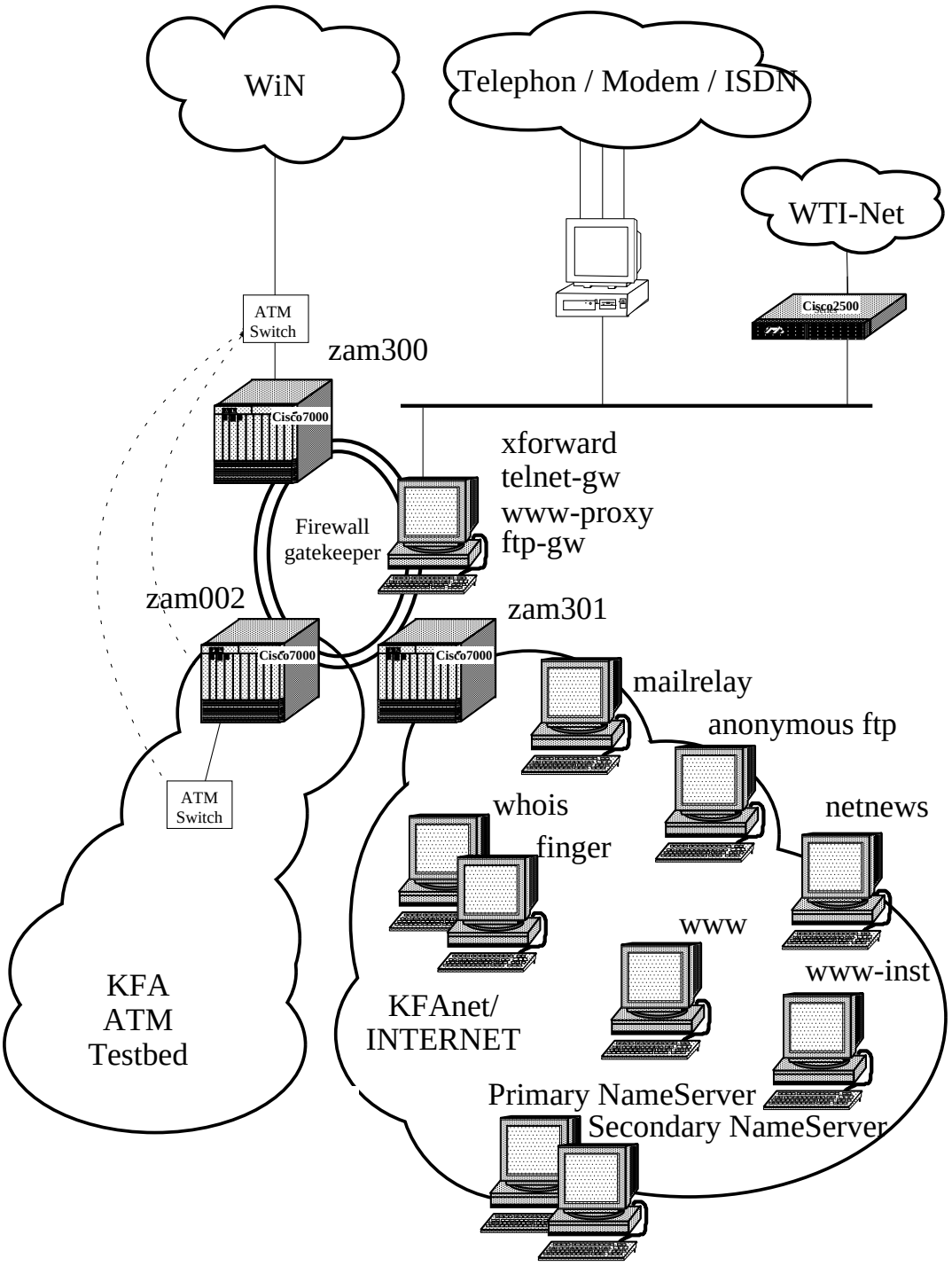


Abb. 25: Schematisches Firewall Netz-Layout

7.14 Eine Lösung für die KFA

Im vorigen Abschnitt haben wir darauf hingewiesen, daß nicht alle Server zwingend auf unterschiedlichen Systemen zur Verfügung gestellt werden müssen. Das Nutzungsprofile der einzelnen Server (Benutzerlast, I/O-Nutzung, Netzlast, CPU-Verbrauch etc.) legt nahe bestimmte Server zusammenzulegen. So hat die Erfahrung gezeigt, daß z.B. das Mail-Relay auf einem getrennten Rechner installiert werden sollte, da hohe I/O-Last und CPU-Last gleichzeitig auftreten, während z.B. Fingerd, Whoisd und NetNewsd auf einem gemeinsamen System ohne sichtbare Performance-Einbußen laufen könnten. Anonymous FTP und WWW können voraussichtlich auch auf einem gemeinsamen System implementiert werden. Vorerst scheint es sinnvoll aufgrund der nicht allzu hohen Last auch den NetNews Server hier noch mit zu integrieren.

8 Käufliche Firewall Produkte

Derzeit werden am Markt eine ganze Reihe von käuflichen Firewall Produkten angeboten. Vergleiche hierzu im Anhang das Kapitel "*Commercial Firewalls and partial FW products*". Leider bieten diese Produkte oft nicht das, was sie auf den ersten Blick versprechen. Meist sind sie nur für kleinere Installationen oder Installationen mit geringem Datendurchsatz geeignet. Firewall-Produkte, die einen externen Anschluß mit 34 Mbit/s unterstützen sind derzeit noch nicht verfügbar.

IBM z.B. weist bereits im ersten Satz seines Announcements darauf hin, daß interne Benutzer mit IBM NetSP Secured Network Gateway Version 1.2 begrenzten Verkehr mit externen Benutzer haben können.

IBM bietet mit *NetSP Secured Network Gateway Version 1.2* [IBM-1], [IBM-2], [IBM-3]

- Proxy oder Application Gateways für ftp und Telnet
- Remote API (*SOCKS*) Server, Socksified Clients für AIX für die Applikationen *Telnet, FTP, Finger* und *Whois* werden mitgeliefert. Public Domain socksified Gopher und Mosaic Clients wurden erfolgreich mit dem NetSP firewall getestet. Ein AIX Gopher und AIX Mosaic Client steht mittels anonymous FTP zur Verfügung.[5]
- Filtern von IP-Paketen
- Für die Authentisierung von Benutzern können Digital Pathways SecureNet Key-Cards und Security Dynamics SecurID Cards benutzt werden.

DEC bietet mit *SEAL (Internet Security: Screening External Access Link)* bzw. *Firewall Service for DEC OSF/1* einem Unternehmen

- Security Unterstützung,
- Entwicklung einer Internet Security Policy,
- Installation und Konfiguration von Softwarekomponenten und
- ein Training für Mitarbeiter des Unternehmens

Die angebotene Software bietet eine Menge von Application Gateways (E-Mail, FTP, Archie, Telnet, Gopher, Mosaic und NetNews). Zugangskontrolle wird auf User-Ebene realisiert.

Zusätzlich können geordert werden:

- weitere Applikation Gateways
- Konfiguration einer Public Domain SOCKS Software
- Kryptographie und Authentication Devices.

SUN bietet mit *Firewall-1* Version 1.2 ein Produkt der Firma CheckPoint Software Technologies Ltd an. Laut Werbeprospekt liest sich dies so:

- Verhindert unerlaubten Zugriff
- Dynamische "Filter" Technologie auf Application Level
- User Authentication (Zugangskontrolle)
- Volle Sicherheit für Netzwerk und Anwender

[5] ftp://ftp.nec.com/pub/security/socks.cstc

- Leistungsstarke Protokollierung und Alarmierung
- Anspruchsvolles GUI für einfache Installation, Verwaltung und Kontrolle
- “Unsichtbar” für Anwender und Applikationen
- Anpassungsfähig bei Veränderungen der Netzwerktopologie, Protokolle und Anwendungen
- Erweiterbar auf unternehmensweite interne und externe Netzwerksicherheit

Firewall-1 ist ein sogenanntes Packet-Filter-Gateway. Durch die Konstruktion *virtueller Verbindungen* hat man vollständige Kontrolle über die gesamte Netzwerk-Kommunikation. UDP-Verkehr ist hier möglich, also z.B. auch NFS. Nachteilig ist hier jedoch, daß dann sämtlicher Verkehr überwacht werden muß, d.h. alle Pakete müssen durch das *Firewall-1*–Gateway. Eine Lastaufteilung auf Protokoll-Ebene ist hier nicht möglich.

TIS (Trusted Information Systems Inc) bietet zwei Produkte an. Das Produkt Gauntlet ist käuflich und besteht aus einem Hardware- und einem Softwareteil. Gauntlet ist ein Rechner-basiertes Firewall, das Application Gateways für Telnet/Rlogin, FTP, E-Mail, NetNews, WWW, XWindow und Gopher zur Verfügung stellt. Allgemein bietet es:

- Application Gateways
- User Authentication (Software- und Token-basierte One-Time-Passwords)
- Firewall System Integrity Checker
- Alarmierungsfunktionen
- Auditing Tools (RealTime und Request-gesteuert)

TIS liefert mit dem Produkt Gauntlet auch den Source-Code. Hierdurch kann man erstens das Produkt auf Besonderheiten in der eigenen Installation zuschneiden, und zweitens bei Software-Bugs schnellstmöglich reagieren.

Das zweite Produkt, das von **TIS** (Trusted Information Systems Inc) angeboten wird, ist ein lizensiertes, aber kostenlos erhältliches Paket (nicht Public Domain), bestehend aus einer Menge von Programmen und Konfigurationspraktiken zum einfacheren Konstruieren eines Firewalls. Dieses Produkt wird allgemein als das *TIS Firewall Toolkit* (TIS fwtk) bezeichnet.

Die Software ist so konzipiert, das Einzelkomponenten zu einer auf die einzelne Installation zugeschnittenen Gesamtlösung zusammengefügt werden können. Das Toolkit bietet somit keine schlüsselfertige Lösung. Die Software ist lauffähig unter UNIX mit TCP/IP und einem BSD-Style Socket Interface.

Die Installation des Toolkits erfordert praktische Erfahrung mit der UNIX Administration und TCP/IP Networking.

Als Application-Level-Gateways stehen zur Verfügung:

- Smap (E-Mail–Application Gateway, SMTP Service)
- Telnet, Rlogin
- FTP,
- HTTP– und X-Application-Gateway
- Plug-Gateway (General purpose Proxy-Server, ein Stück Software, mit dem verschiedenste Anwendungen *zusammengestöpselt* werden können. Z.B. kann ein NetNews-Client über ein Plug-Gateway mit einem NetNews Server kommunizieren.)

Weitere Komponenten sind:

- Authd (Network Authentication Service)
- Telnetd to Firewall (Network Login to the Firewall)
- Login – User Authentication für z.B.
  - Digital Pathways SecureNet KeyCards,
  - Security Dynamics SecurID Cards und
  - Racal Watchword
- ftpd (secured Anonymous FTP Service)
- Syslogd (erweiterter System Logging Daemon)
- User Authentication (Software- und Token-basierte One-Time-Passwords)
- Firewall System Integrity Checker
- Alarmierungsfunktionen
- Auditing Tools (RealTime und Request-gesteuert)

Da das TIS fwtk ein selbst zu übersetzendes und installierendes Produkt ist, hat man auch hier den Vorteil, der sich aus der Verfügbarkeit des Source-Codes ergibt.

10 Die Umsetzung in die Praxis

Die Implementierung des bisher beschriebenen Firewall-Konzeptes läßt sich leicht durchführen.

Die Software-Komponenten der Firma Trusted Information Systems (TIS fwtk) für das Telnet, FTP, HTTP und X-Applikations-Gateway konnten nach kleineren Modifikationen problemlos auf einer DEC 3000 M300 Workstation übersetzt und in Betrieb genommen werden.

Die Filterregeln für den Firewall Router *zam301* könnten als Access-Liste per TFTP in den Router übernommen werden.

Eine zusätzliche Filterregel, die Rechnern im DialUp-Netz (Telephon, Modem, ISDN) verbietet, direkten Zugang zum internen Netz durchzuführen, ist leicht integrierbar. Diese Rechner können dann nur noch wie externe Rechner über den Firewall nach intern kommunizieren.

Interne WWW, Anonymous-FTP, Mail und NetNews-Server sind bereits vorhanden, brauchen somit nicht zusätzlich installiert zu werden. Interne Whois und Finger-Server werden derzeit nicht benötigt.

Eine wirkliche Implementierung des Sicherheits-Konzeptes scheint also derzeit nur an der Akzeptanz der Benutzer zu scheitern, die zu einer Einschränkung ihrer jetzigen Kommunikationsmöglichkeiten nicht bereit zu sein scheinen.

11 Schlußbemerkungen

In diesem Bericht wurde versucht die Gefahren, die durch ein Firewall eingeschränkt werden können, zu erörtnern. Nichtsdestotrotz sollte an dieser Stelle nicht verschwiegen werden, daß es weitere Angriffspunkte gibt, die auch durch ein Firewall nicht abgedeckt werden können.

Es werden Gelder in Millionenhöhe für Sicherheitsmaßnahmen, deren Erforschung und Entwicklung ausgegeben. Diese Maßnahmen dienen dazu, unauthorisierten Personen Zugriff auf die Computersysteme zu verweigern.

Ein Sicherheitsbereich wird jedoch gänzlich vernachlässigt. Dieser wird allgemein als *Social Engineering* bezeichnet. Social Engineering ist allgemein der Prozess des Informationsgewinns auf soziale, interaktive Weise. Vereinfacht dargestellt, ruft ein Hacker, getarnt als Mitarbeiter der Systemwartung, bei einem anderen, meist neuem, unerfahrenen Mitarbeiter an und fragt nach dem Passwort des Benutzers. Die Informationen hierzu, sich als z.B. Sicherheitsbeauftragter oder Systemadministrator zu tarnen, erhält er über Telephonlisten, WWW-Informationen, Veröffentlichungen, ... Eine Attacke über weniger als drei Tage bei einem amerikanischen Unternehmen brachte soviele Informationen zu Tage, daß jedes Hard- und Software-mäßige Sicherheitssystem umgangen werden konnte. Vergleiche hierzu weiter unten das Schaubild *Anatomie einer Attacke mittels Social Engineering* [Winkler,I.S., Dealy,B.].

Wenn Sicherheitsfragen mit der Benutzbarkeit eines Systems interferieren, werden Benutzer versuchen diese zu umgehen. Viele Sicherheitssysteme versagen, weil ihre Designer nicht den menschlichen Faktor berücksichtigt haben. Automatisch generierte Passwörter werden aufgeschrieben, da man sie sich nicht merken kann. Türen bleiben auf, da vergessen wurde sie abzuschließen.

Hier muß es Aufgabe eines Computer-Sicherheitsbeauftragten sein, daß nötige Sicherheitsbewußtsein bei den Benutzern zu schüren. Investitionen in beträchtlicher Höhe stehen hier auf dem Spiel, ohne daß dem bisher Rechnung getragen wird.

Security-Policies sind lebende Gebilde. Organisationen ändern sich, neue Protokolle entstehen oder werden erweitert. Security-Policies müssen ständig angeglichen und eventuell ausgetauscht werden, um den neuen Gegebenheiten, neue Geschäftspolitik, technologische Änderungen und Veränderungen in der Ressource-Ausnutzung, Rechnung zu tragen.

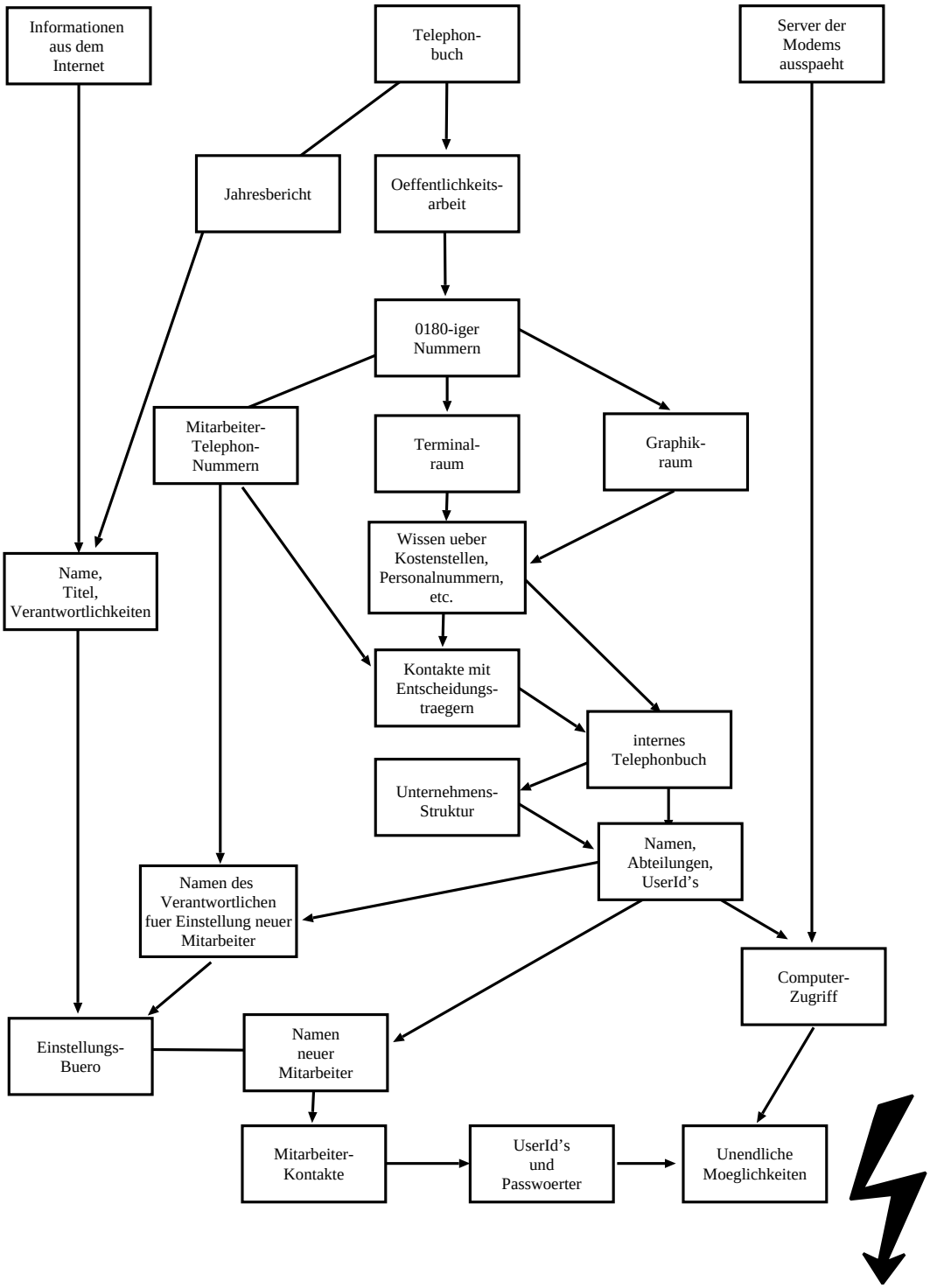


Abb. 26: Anatomie einer Attacke mittels *Social Engineering*[6]

[6] [Winkler,I.S., Dealy,B.]

12 Ein Leben ohne Firewall[7]

Was ist zu tun, wenn kein Firewall installiert werden kann? Was kann man tun, um sich selbst zu schützen?

Grundsätzlich sollten alle standardmäßigen Host-Sicherheitsmechanismen genutzt werden. Dies ist sicherlich auch bei der Benutzung eines Firewalls dringend zu empfehlen, muß jedoch ohne Firewall mit mehr Sorgfalt und für wesentlich mehr Maschinen durchgeführt werden. Um Passwort-Benutzung anderer zu vermeiden, sollten Programme wie S/Key genutzt werden.

Eine zweite Antwort auf die Frage bedeutet, alle Basis-Sicherheitsprinzipien anzuwenden. Nicht alle Dienste müssen auf allen Systemen angeboten werden. Eine sorgfältige Analyse wird eine Reihe von Diensten ergeben, die abgeschaltet werden können oder nur eingeschränkt zur Verfügung gestellt zu werden brauchen.

Der TFTP-Dienst wird beispielsweise meist nur zum *Booten* von Diskless Workstations, X-Terminals oder ähnlichem benötigt. Das bedeutet aber nicht, daß der Rest der Welt diesen Services auch nutzen (können) muß. Dies kann mittels eines Filtering Routers oder von TCP Wrapper Programmen verhindert werden.

Andere Dienste sollten ähnlich behandelt werden. Auf vielen Maschinen wird sicherlich kein *ftpd* benötigt, auf diesen kann dieser Dienst abgeschaltet werden. CERT veröffentlicht eine Liste von sogenannten *gefährlichen Ports*. Diese sollten an der Eingangstür abgeblockt werden.

Filter-Regeln müssen nicht statisch sein. Wenn jemand zeitweise externe Anbindung benötigt, können notwendige Dienste für diese Zeit geöffnet werden, so kann z.B. X11 für bestimmte Maschinen zu bestimmten Zeiten freigegeben werden. Grundsätzlich sollte man jedoch bei solchen *temporären* Lösungen vorsichtig sein. Ein formaler Mechanismus sollte hierzu etabliert werden.

Letztendlich sollte man sich sicher sein, welche Maschinen wirklich sicher sind. Das eigene Subnetz mag sicher sein, aber wenn rlogins von außerhalb zugelassen werden, kann die eigene Maschine von dort über einen indirekten Pfad kompromittiert werden. Wiederum sollten Packet Filter, Wrapper Programme und ein Verbot von *.rhosts* Dateien genutzt werden.

“Sure, I’m paranoid.
But am I paranoid enough?

The Firewall manager

[7] Dieses Kapitel wurde frei übersetzt von [Cheswick, Bellovin] übernommen.

13.1 Firewalls Frequently Asked Questions (FAQ's)[8]

About the FAQ

This FAQ is not an advertisement or endorsement for any product, company, or consultant. The maintainer welcomes input and comments on the contents of this FAQ. Comments related to the FAQ should be addressed to Fwalls-FAQ@tis.com.

13.1.1 What is a network firewall?

A firewall is any one of several ways of protecting one network from another untrusted network. The actual mechanism whereby this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.

13.1.2 Why would I want a firewall?

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spraypaint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. A firewall's purpose is to keep the jerks out of your network while still letting you get your job done.

Many traditional-style corporations and data centers have computing security policies and practices that must be adhered to. In a case where a company's policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy. Frequently, the hardest part of hooking to the Internet, if you're a large company, is not justifying the expense or effort, but convincing management that it's safe to do so. A firewall provides not only real security - it often plays an important role as a security blanket for management.

Lastly, a firewall can act as your corporate "ambassador" to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and so forth. Several of these systems have become important parts of the Internet service structure (e.g.: UUnet.uu.net, gatekeeper.dec.com) and have reflected well on their corporate sponsors.

13.1.3 What can a firewall protect against?

Some firewalls permit only Email traffic through them, thereby protecting the network against any attacks other than attacks against the Email service. Other firewalls provide less strict protections, and block services that are known to be problems.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. This, more than anything, helps prevent vandals from logging

[8] Entnommen aus: *ftp://ftp.greatcircle.com/pub/firewalls/FAQ*

into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against any type of network borne attack if you unplug it.

Firewalls are also important since they can provide a single "choke point" where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective "phone tap" and tracing tool.

13.1.4 What can't a firewall protect against?

Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data. Firewall policies must be realistic, and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack – attacks in which something is mailed or copied to an internal host where it is then executed. This form of attack has occurred in the past against various versions of Sendmail.

13.1.5 What are good sources of print information on firewalls?

There are several books that touch on firewalls. The best known are:

Cheswick and Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker" Addison-Wesley, April, 1994 ISBN 0-201-63357-4 Garfinkel and Spafford, "Practical UNIX Security" O'Reilly and associates (discusses primarily host security)

Related references are:

Comer and Stevens, "Internetworking with TCP/IP" Prentice Hall, 1991 Curry, "UNIX System Security" Addison Wesley, 1992

13.1.6 Where can I get more information on firewalls on the network?

Ftp.greatcircle.com - Firewalls mailing list archives. Directory: pub/firewalls Ftp.tis.com - Internet firewall toolkit and papers. Directory: pub/firewalls Research.att.com - Papers on firewalls and breakins. Directory: dist/internet_security Net.Tamu.edu - Texas AMU security tools. Directory: pub/security/TAMU

The internet firewalls mailing list is a forum for firewall administrators and implementors. To subscribe to Firewalls, send "subscribe firewalls" in the body of a message (not on the "Subject:" line) to "Majordomo@GreatCircle.COM". Archives of past Firewalls postings are available for anonymous FTP from ftp.greatcircle.com in pub/firewalls/archive

13.1.7 What are some commercial products or consultants who sell/service firewalls?

We feel this topic is too sensitive to address in a FAQ, as well as being difficult to maintain an up-to-date list.

13.1.8 What are some of the basic design decisions in a firewall?

There are a number of basic design issues that should be addressed by the lucky person who has been tasked with the responsibility of designing, specifying, and implementing or overseeing the installation of a firewall.

The first and most important is reflects the policy of how your company or organization wants to operate the system: is the firewall in place to explicitly deny all services except those critical to the mission of connecting to the net, or is the firewall in place to provide a metered and audited method of "queuing" access in a non-threatening manner. There are degrees of paranoia between these positions; the final stance of your firewall may be more the result of a political than an engineering decision.

The second is: what level of monitoring, redundancy, and control do you want? Having established the acceptable risk level (e.g.: how paranoid you are) by resolving the first issue, you can form a checklist of what should be monitored, permitted, and denied. In other words, you start by figuring out your overall objectives, and then combine a needs analysis with a risk assessment, and sort the almost always conflicting requirements out into a laundry list that specifies what you plan to implement.

The third issue is financial. We can't address this one here in anything but vague terms, but it's important to try to quantify any proposed solutions in terms of how much it will cost either to buy or to implement. For example, a complete firewall product may cost between $100,000 at the high end, and free at the low end. The free option, of doing some fancy configuring on a Cisco or similar router will cost nothing but staff time and cups of coffee. Implementing a high end firewall from scratch might cost several man-months, which may equate to $30,000 worth of staff salary and benefits. The systems management overhead is also a consideration. Building a home-brew is fine, but it's important to build it so that it doesn't require constant and expensive fiddling-with. It's important, in other words, to evaluate firewalls not only in terms of what they cost now, but continuing costs such as support.

On the technical side, there are a couple of decisions to make, based on the fact that for all practical purposes what we are talking about is a static traffic routing service placed between the network service provider's router and your internal network. The traffic routing service may be implemented at an IP level via something like screening rules in a router, or at an application level via proxy gateways and services.

The decision to make here is whether to place an exposed stripped-down machine on the outside network to run proxy services for telnet, ftp, news, etc., or whether to set up a screening router as a filter, permitting communication with one or more internal machines. There are plusses and minuses to both approaches, with the proxy machine providing a greater level of audit and potentially security in return for increased cost in configuration and a decrease in the level of service that may be provided (since a proxy

needs to be developed for each desired service). The old trade-off between ease-of-use and security comes back to haunt us with a vengeance.

13.1.9 What are proxy servers and how do they work?

A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet. Proxies are often used instead of router-based traffic controls, to prevent traffic from passing directly between networks. Many proxies contain extra logging or support for user authentication. Since proxies must "understand" the application protocol being used, they can also implement protocol specific security (e.g., an FTP proxy might be configurable to permit incoming FTP and block outgoing FTP).

Proxy servers are application specific. In order to support a new protocol via a proxy, a proxy must be developed for it. SOCKS is a generic proxy system that can be compiled into a client-side application to make it work through a firewall. Its advantage is that it's easy to use, but it doesn't support the addition of authentication hooks or protocol specific logging. For more information on SOCKS, see ftp.nec.com: /pub/security/socks.cstc Users are encouraged to check the file "FILES" for a description of the directory's contents.

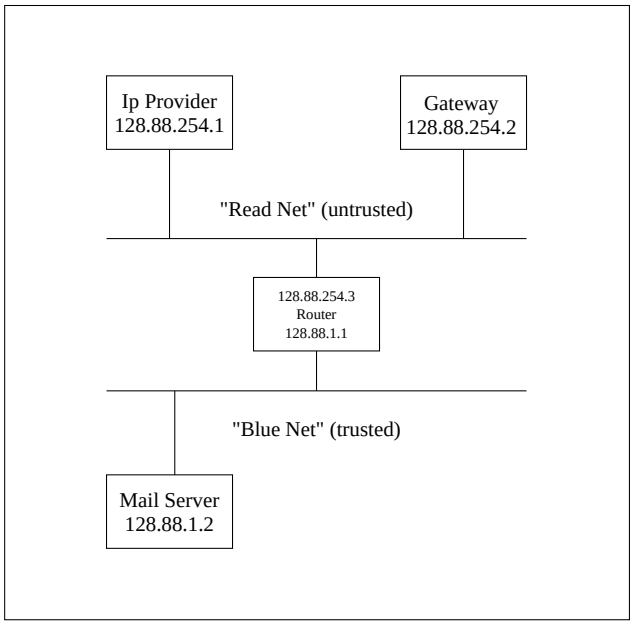
13.1.10 What are some cheap packet screening tools?

The Texas AMU security tools include software for implementing screening routers (FTP net.tamu.edu, pub/security/TAMU). Karlbridge is a PC-based screening router kit (FTP nisca.acs.ohio-state.edu, pub/kbridge). A version of the Digital Equipment Corporation "screend" kernel screening software is available for BSD/386, NetBSD, and BSDI. Many commercial routers support screening of various forms.

13.1.11 What are some reasonable filtering rules for my Cisco?

The following example shows one possible configuration for using the Cisco as a filtering router. It is a sample that shows the implementation of a specific policy. Your policy will undoubtedly vary.

In this example, a company has Class B network address of 128.88.0.0 and is using 8 bits for subnets. The Internet connection is on the "red" subnet 128.88.254.0. All other subnets are considered trusted or "blue" subnets.



Keeping the following points in mind will help in understanding the configuration fragments:

- Ciscos applying filtering to output packets only.
- Rules are tested in order and stop when the first match is found.
- There is an implicit deny rule at the end of an access list that denies everything.

The example below concentrates on the filtering parts of a configuration. Line numbers and formatting have been added for readability.

The policy to be implemented is:

- Anything not explicitly allowed is denied
- Traffic between the external gateway machine and blue net hosts is allowed.
- permit services orginating from the blue net
- allow a range of ports for FTP data connections back to the blue net.

- 1 no ip source-route
- 2 !
- 3 interface Ethernet 0
- 4 ip address 128.88.1.1 255.255.255.0
- 5 ip access-group 10
- 6 !
- 7 interface Ethernet 1
- 8 ip address 128.88.254.3 255.255.255.0
- 9 ip access-group 11
- 10 !
- 11 access-list 10 permit ip 128.88.254.2 0.0.0.0 128.88.0.0 0.0.255.255
- 12 access-list 10 deny tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 lt 1025
- 13 access-list 10 deny tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 gt 4999

- 14 access-list 10 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255
- 15 !
- 16 access-list 11 permit ip 128.88.0.0 0.0.255.255 128.88.254.2 0.0.0.0
- 17 access-list 11 deny tcp 128.88.0.0 0.0.255.255 0.0.0.0 255.255.255.255 eq 25
- 18 access-list 11 permit tcp 128.88.0.0 0.0.255.255 0.0.0.0 255.255.255.255

Lines Explanation

- 1 Although this is not a filtering rule, it is good to include here.
- 5 Ethernet 0 is on the red net. Extended access list 10 will be applied to output on this interface. You can also think of output from the red net as input on the blue net.
- 9 Ethernet 1 is on the blue net. Extended access list 11 will be applied to output on this interface.
- 11 Allow all traffic from the gateway machine to the blue net.
- 12-14 Allow connections originating from the red net that come in between ports 1024 and 5000. This is to allow ftp data connections back into the blue net. 5000 was chosen as the upper limit as it is where OpenView starts.

Note: again, we are assuming this is acceptable for the given policy. There is no way to tell a Cisco to filter on source port. Newer versions of the Cisco firmware will apparently support source port filtering.

Since the rules are tested until the first match we must use this rather obtuse syntax.

- 16 Allow all blue net packets to the gateway machine.
- 17 Deny SMTP (tcp port 25) mail to the red net.
- 18 Allow all other TCP traffic to the red net.

Cisco.Com has an archive of examples for building firewalls using Cisco routers, available for FTP from: ftp.cisco.com in /pub/acl-examples.tar.Z

13.1.12 How do I make DNS work with a firewall?

Some organizations want to hide DNS names from the outside. Many experts disagree as to whether or not hiding DNS names is worthwhile, but if site/corporate policy mandates hiding domain names, this is one approach that is known to work.

This approach is one of many, and is useful for organizations that wish to hide their host names from the Internet. The success of this approach lies on the fact that DNS clients on a machine don’t have to talk to a DNS server on that same machine. In other words, just because there’s a DNS server on a machine, there’s nothing wrong with (and there are often advantages to) redirecting that machine’s DNS client activity to a DNS server on another machine.

First, you set up a DNS server on the bastion host that the outside world can talk to. You set this server up so that it claims to be authoritative for your domains. In fact, all this server knows is what you want the outside world to know; the names and addresses of your gateways, your wildcard MX records, and so forth. This is the "public" server.

Then, you set up a DNS server on an internal machine. This server also claims to be authoritiative for your domains; unlike the public server, this one is telling the truth. This is your "normal" nameserver, into which you put all your "normal" DNS stuff. You

also set this server up to forward queries that it can't resolve to the public server (using a "forwarders" line in /etc/named.boot on a UNIX machine, for example).

Finally, you set up all your DNS clients (the /etc/resolv.conf file on a UNIX box, for instance), including the ones on the machine with the public server, to use the internal server. This is the key.

An internal client asking about an internal host asks the internal server, and gets an answer; an internal client asking about an external host asks the internal server, which asks the public server, which asks the Internet, and the answer is relayed back. A client on the public server works just the same way. An external client, however, asking about an internal host gets back the "restricted" answer from the public server.

This approach assumes that there's a packet filtering firewall between these two servers that will allow them to talk DNS to each other, but otherwise restricts DNS between other hosts.

Another trick that's useful in this scheme is to employ wildcard PTR records in your IN-ADDR.ARPA domains. These cause an an address-to-name lookup for any of your non- public hosts to return something like "unknown.YOUR.DOMAIN" rather than an error. This satisfies anonymous FTP sites like ftp.uu.net that insist on having a name for the machines they talk to. This may fail when talking to sites that do a DNS cross-check in which the host name is matched against its address and vice versa.

Note that hiding names in the DNS doesn't address the problem of host names "leaking" out in mail headers, news articles, etc.

13.1.13 How do I make FTP work through my firewall?

Generally, making FTP work through the firewall is done either using a proxy server or by permitting incoming connections to the network at a restricted port range, and otherwise restricting incoming connections using something like "established" screening rules. The FTP client is then modified to bind the data port to a port within that range. This entails being able to modify the FTP client application on internal hosts.

A different approach is to use the FTP "PASV" option to indicate that the remote FTP server should permit the client to initiate connections. The PASV approach assumes that the FTP server on the remote system supports that operation. (See RFC1579 for more information)

Other sites prefer to build client versions of the FTP program that are linked against a SOCKS library.

13.1.14 How do I make Telnet work through my firewall?

Telnet is generally supported either by using an application proxy, or by simply configuring a router to permit outgoing connections using something like the "established" screening rules. Application proxies could be in the form of a standalone proxy running on the bastion host, or in the form of a SOCKS server and a modified client.

13.1.15 How do I make Finger and whois work through my firewall?

Permit connections to the finger port from only trusted machines, which can issue finger requests in the form of: finger user@host.domain@firewall

This approach only works with the standard UNIX version of finger. Some finger servers do not permit user@host@host fingering.

Many sites block inbound finger requests for a variety of reasons, foremost being past security bugs in the finger server (the Morris internet worm made these bugs famous) and the risk of proprietary or sensitive information being revealed in user's finger information.

13.1.16 How do I make gopher, archie, and other services work through my firewall?

This is still an area of active research in the firewall community. Many firewall administrators support these services only through the character-cell interface provided by telnet. Unfortunately, many of the sexier network services make connections to multiple remote systems, without transmitting any inline information that a proxy could take advantage of, and often the newer information retrieval systems transmit data to local hosts and disks with only minimal security. There are risks that (for example) WAIS clients may request uuencoded files, which decode and modify security related files in the user's home directory. At present, there is a lot of head-scratching going on between the firewall administrators who are responsible for guarding the network perimeters, and the users, who want to take advantage of these very sexy and admittedly useful tools.

13.1.17 What are the issues about X-Window through a firewall?

X Windows is a very useful system, but unfortunately has some major security flaws. Remote systems that can gain or spoof access to a workstation's X display can monitor keystrokes that a user enters, download copies of the contents of their windows, etc.

While attempts have been made to overcome them (E.g., MIT "Magic Cookie") it is still entirely too easy for an attacker to interfere with a user's X display. Most firewalls block all X traffic. Some permit X traffic through application proxies such as the DEC CRL X proxy (FTP crl.dec.com).

13.1.18 Glossary of firewall related terms

Host-based Firewall: A firewall where the security is implemented in software running on a general-purpose computer of some sort. Security in host-based firewalls is generally at the application level, rather than at a network level. Router-based Firewall: A firewall where the security is implemented using screening routers as the primary means of protecting the network. Screening Router: A router that is used to implement part of the security of a firewall by configuring it to selectively permit or deny traffic at a network level. Bastion Host: A host system that is a "strong point" in the network's security perimeter. Bastion hosts should be configured to be particularly resistant to attack. In a host-based firewall, the bastion host is the platform on which the firewall software is run. Bastion hosts are also referred to as "gateway hosts." Dual-Homed Gateway: A firewall consisting of a bastion host with 2 network interfaces, one of which is connected to the protected network, the other of which is connected to the Internet. IP traffic forwarding is usually disabled, restricting all traffic between the two networks to whatever passes through some kind of application proxy. Application Proxy: An application that forwards application traffic through a firewall. Proxies tend to be specific to the protocol they

are designed to forward, and may provide increased access control or audit. Screened Subnet: A firewall architecture in which a "sand box" or "demilitarized zone" network is set up between the protected network and the Internet, with traffic between the protected network and the Internet blocked. Conceptually, this is similar to a dual-homed gateway, except that an entire network, rather than a single host is reachable from the outside.

Contributors:

mjr@tis.com - Marcus Ranum, Trusted Information Systems

leibowa@wl.com - Allen Leibowitz, Warner Lambert Inc.

brent@greatcircle.com - Brent Chapman, Great Circle Associates

bdboyle@erenj.com - Brian Boyle, Exxon Research

13.2 A Brief History of the TAMU Incidents[9]

On Tuesday 25 August 1992, the Texas A&M University Supercomputer Center (TAMUSC) was notified by the Ohio Supercomputer Center that a specific TAMU machine was being used to attack one of their computers over internet. The local machine turned out to be a Sun workstation in a faculty member's office. Unfortunately, this faculty member was out of town for a week, so rather than trying to convince the department head to let us in without the faculty present, we decided to monitor network connections to the workstation, and if necessary, disconnect the machine from the net electronically. This decision to monitor the machine's sessions rather than immediately securing it turned out to be very fortunate, as this monitoring gave us a wealth of information about the intruders and their methods.

The initial monitoring tools were very simple, but as the significance of what we were seeing became apparent, we rapidly improved the tools to the point that we were able to watch the intruder's entire session in real time, keystroke by keystroke. This monitoring led to the discovery that several outside intruders were involved, and that many other local machines had been compromised. One local machine had even been set up as a cracker bulletin board machine, that the crackers would use to contact each other and discuss techniques and progress!

By Thursday 27 August, there was enough information about which machines had been compromised, and how they had been broken into, that we could effectively clean them up. In addition, the severity of the modifications the intruders were making, particularly on the bulletin board machine, made it imperative to stop the intrusions, so we contacted the respective system managers, and arranged to shut down all machines, and scheduled the system cleanup for the next day.

On Friday 28 August, we worked on the known affected machines, closing the security holes that had been used to break in, and brought them all back up on the network.

On Saturday 29 August, an emergency call was received from one of the system managers, saying that the intruders had broken back into the cracker bulletin board machine. Concerned about the integrity of their research data, they asked for their machines to be physically disconnected from the rest of the network.

On Monday 31 August, the logs of the new break-in were ananlyzed, and it was determined that the crackers were much more sophisticated than originally believed and that many more local machines and user accounts had been compromised than initially realized. Several files were found containing hundreds of captured passwords including ones on major (supposedly secure) servers. It appeared that there were actually two levels of crackers. The high level were the more sophisticated with a thorough knowledge of the technology; the low level were the "foot soldiers" who merely used the supplied cracking programs with little understanding of how they worked. Our initial response had been based on watching the later, less capable crackers, and was insufficient to handle the more sophisticated ones.

After much deliberation, it was decided that the only way to protect the computers on campus was to block certain key incoming network protocols, reenabling them to local

[9] Entnommen aus [Safford, Schales, Hess-1], TAMU —Texas A&M University

machines on a case by case basis, as each machine had been cleaned up and secured. The rationale was that if the crackers had access to even one unsecure local machine, it could be used as a base for further attacks, so we had to assume all machines had been compromised, unless proven otherwise.

The recommendation to filter incoming traffic was presented to the Associate Provost for Computing on Monday afternoon, and approved. The necessary equipment for the filter and monitor machines was bought or borrowed late that afternoon, and the design and coding of the filterproceeded through the night. Particular effort was made in the design to achieve the necessary security with the minimum of impact to local users. The filter was completed and installed by 5PM Tuesday 1 September.

At this point, the major task of analyzing all of the detailed logs and captured files was restarted. It was discovered that over 40MB of the cracker's tools had been captured, tolls that they had FTP'ed onto some of the broken machines. These tools included Crack, network monitoring tools, all SunOS, Ultrix and Dynix source code (so they could replace any executable on the system), and cracking programs for virtually every CERT announced vulnerability. The logs showed that the crackers routinely placed back door and trojan login binaries on each broken system and used programs to set the timestamp anmd checksum of the replaced binaries to avoid detection.

On Thursday 3 September, TAMUSC monitor logs showed an obviously automated attack by ftp that was sequentially probing every machine on campus. Here again it was decided to monitor this attack, as it was not clear what it could accomplish. This decision to observe, rather than immediately block, turned out to be very fortunate.

Shortly after midnight on Friday, 4 September, TAMUSC received a report from another site via the Computing Emergency Response Team (CERT) at Carnegie Mellon that the crackers had broken back into TAMU machines. The logs were immediately analyzed, and it was determined that the crackers had used ftp to install a program that allowed them to tunnel past the TAMU filter's blocks. In addition, even though they knew we were aware of their origional intrusions, they continued their pattern of breaking in and replacing key system binaries.

At this point, the filter was completely redesigned to keep the crackers out, and installed the new version by 5AM Saturday. The new version changed the filter approach from "deny" based filtering (let everything in unless it is specifically denied) to "allow" based filtering (block everything unless it is specifically allowed). this new version, while providing much greater security, was unfortunately also more visible to valid users.

Since the new filter was installed, no successful intrusion attacks against TAMU machines have been observed, despite continued logging of probes and continued attempts. Recent efforts have centered in three areas: improving the ease of use and throughput of the filter, reducing the manpower requirements of the monitoring tools, and developing a program to help local system managers check their machines for proper security configuration.

13.3 Commercial Firewalls and partial FW products[10]

Maintained by Catherine Fulmer

BlackHole "BlackHole": Check http://www.milkway.com for the info. David Cross, Vice-President, Sales, Milkyway Networks Corporation, The home of the Balck Hole firewall, Ottawa, Ontario Canada, Voice: (613) 566-4574, Fax: (613) 596-5615 E-mail to: David Cross

Brimstone Brimstone : by SOS.

Cyberguard Cyberguard : Harris Computer Systems Firewall. It runs on a PC tower Chassis with a Night Hawk 4800 series CPU board (Motorola 88100-based), CX/SX operating system and LAN/SX networking. The OS and networking systems are "NCSC B1-level evaluated and ITSEC FB1 E3" secure. To talk to Computer Systems about the product, e-mail nhnews@csd.harris.com or call (305) 974-1700 Ext. 5144 for Sales or Ext. 5124 for Marketing Communications.

DBF DBF by NSC Network Systems Corp. (NSC) has announced a security product called "Data Privacy Facility" (DPF). It encrypts IP datagrams on a per-packet basis, gives you the ability to select what gets encrypted and what doesn't. DPF supports DES, IDEA, and NSC1 encryption algorithms, MD5 for digi-signatures, uses RSA and Diffie/Hellman for key exchange, works great, lasts long time. DPF runs on a router (which means that you can not only encrypt traffic but establish/ control access policy as well.) There is no limit to the number of end-stations that can use an encrypted tunnel. Encrypted packets can be forwarded over any data-link that supports IP (frame relay, ATM, ethernet, T/R, etc.) Network Systems can be contacted at 1-612-424-1488 or by http://www.network.com

Eagle NSMS Eagle from Raptor Systems. *The Eagle Network Security Management System* is a complete, failsafe approach to network security. It overcomes the problems and limitations of less robust approaches through an integrated security architecture. The Eagle runs on a dedicated IBM, Hewlett-Packard, or Sun workstation. This eliminates the loopholes of traditional firewall solutions that are installed on workstations that support other applications and network users, thus compromising the integrity of the security software. Web: http://www.raptor.com. Email: info@raptor.com Raptor Systems, Inc., 69 Hickory Drive, Waltham, MA 02154, Voice: 617-487-7700 Fax: 617-487-6755

Eaglet SSMS *The Eaglet Subnet Security Management System* The Eaglet (tm) Subnet Security Management System is a complete, fail-safe approach to interdepartmental network security. The Eaglet architecture comprises a suite of software products that resides between partitioned LANs within the enterprise to monitor, control and provide (or restrict) access to network resources. Web: http://www.raptor.com. Email: info@raptor.com

[10] Vergleiche aktuell: [Fulmer,C.]

Raptor Systems, Inc., 69 Hickory Drive, Waltham, MA 02154, Voice: 617-487-7700 Fax: 617-487-6755

ExFilter V1.1.2 ExFilter V1.1.2 for SunOS 4.1.x Security and Internet Gateway Software All-in-one Firewall, Router and Network-manager 80% of major Internet-connected sites have suffered hacking attempts. ExFilter turns a Sun workstation running Solaris 1 (SunOS 4.1.x) into a firewall, router and network-manager. The Sun becomes a secure gateway between your network and the Internet, and between segments of the same network. Email: exfilter@exnet.com or exfilter@exnet.co.uk

Firewall-1 Firewall-1, (by Checkpoint, software only.) Available thru many resellers (see next section). FireWall-1 is protecting hundreds of networks world wide and was reviewd by Open Computing 10/94 and Advanced Systems 12/94. More info: http://WWW.CheckPoint.com info, support, or sales @CheckPoint.com CheckPoint FireWall-1 software is a unique, flexible security system designed to protect your organization against unauthorized access from Internet. The system controls access to your entire organization's heterogeneous network, while providing your users with secure connectivity to all Internet resources and IP based services. It enables a smooth growth path from a single Internet gateway to an enterprise-wide system. CheckPoint FireWall-1 lets you take full control over all Internet gateway traffic. An advanced, patent pending, generic filtering technology inspects each packet, promptly blocking all unwanted communication attempts. A powerful auditing and alerting mechanism identifies and flags any suspicious communication.

Gauntlet Gauntlet by TIS Trusted Information Systems Gauntlet is a hardware- and software-based firewall system designed by Trusted Information Systems, Inc. (TIS), to provide secure access and internetwork communications between private networks and public networks such as the Internet, or between subnets within a private network. Gauntlet offers application- level security services that regulate both incoming and outgoing communications in compliance with established organization security policies. The Gauntlet product includes software based on the popular TIS Internet Firewall Toolkit, and is built on a UNIX operating system configured to restrict access to the private network. Electronic mail to: netsec@tis.com, Web: http://www.tis.com, Telephone: 301-854-6889, Fax to 301-854-5363. Or write to Trusted Information Systems, Inc., ATTN: Network Security, 3060 Washington Road, Glenwood, MD 21738

GFX-94 GFX-94 Internet Firewall The GFX-94 Internet Firewall is a stand alone hardware/software system. The system consists of two hosts systems which create the outer and inner walls of the system, with a private DMZ network between the two. The system provides for network transparency for TCP/IP based applications running behind the firewall. The system admin utility provides for access control over incomming or outgoing packets. System features include domain hiding, mail header

	expunging, one time passwords, SMTP proxy and drop safe logging. The system is provided with 2 ethernet interfaces, one of with can be replaced with an internal router card (56K-T1). Please contact or visit our web pages. Email: info@gta.com, Web: http://www.gta.com, Contact information: Paul Emerson (paul@gta.com), Global Technology Associates, Inc., 3504 Lake Lynda Drive, Suite 160, Orlando, FL 32817, Sales: 1-800-775-4GTA, Tel. +1 407-380-0220, Fax. +1 407-380-6080
Igateway	Igateway by Sun Consulting. Actually called CONSULT-IGATEWAY and consists of telnet and ftp proxies for filtered traffic. Available thru Sun Consulting only.
Integralis	Integralis .... ???
Inter-Ceptor	Inter-Ceptor by Network Security International For info, contact John Shepherd at (516) 674-0238
ANS InterLock	ANS InterLock Service from ANS CO+RE Systems, Inc. For organizations who want to develop and/or enforce network security policies, ANS InterLock application-level service can be customized to meet specific customer requirements and may be used to control access among segments of a private enterprise network and/or to establish a controllable filter between the private network and the public Internet. ANS InterLock service supports telnet, FTP, SMTP, HTTP, Gopher, NNTP, X Window systems, NTP and GPD. ANS Interlock service assures end-to-end service transparency and provides audit logs for resource accounting. The ANS Interlock system can be configured to support end-to-end encryption as well as card key authentication. Access to all services is controlled via the Access Control Rule Base which permits users and/or user groups to access particular services by any combination of userid/password/smartcard, time of day, day of week, inbound or outbound direction, private/public network address and private/public host criteria. These hardware/software solutions offer customers easy administration and strong password management controls. For more information, view our WWW site at: web: http://www.ans.net or contact Sales at: main: 800-456-8267 or 703-758-7700, email: info@ans.net
IRX Router	IRX Router - Livingston Firewall Router This enhanced version of the PortMaster IRX Internetwork Router provides an advanced set of features for attaching a companies network to the world-wide Internet. By providing the most advanced packet filtering available (input and output packet filtering on a per interface basis), the FireWall IRX controls which computers are accessible from the Internet as well as limiting the types of network services those computers can use. For example, the filters can be set to allow electronic mail to and from a companies secure mail host, but block the ability for Internet intruders to establish login sessions to any host computer. Security can also be set up to allow trusted users within a company to directly access information services on the Internet, while denying access to those services from the Internet. Packet logging features allow network administrators to detect and monitor

intruder attempts from the Internet. Contact: info@livingston.com, sales@livingston.com, support@livingston.com. Contact: Joe Sasek, Director of Sales Livingston Enterprises, 6920 Koll Center Parkway #220, Pleasanton, CA 94566, 1-800-458-9966, (510) 426-0770, (510) 426-8951 Fax

JANUS JANUS from Border Network Technologies. The JANUS Firewall Server is the one stop solution to connecting your organization to the Internet. In one highly integrated hardware device, JANUS provides a security Firewall, Internet servers, and an Internet router. The JANUS security Firewall prevents Internet based intruders from accessing your internal networks, while allowing your network users full access to the Internet. JANUS runs all standard Internet servers including a full function electronic mail server with POP and SMTP support, a USENET News server, a Web server, an anonymous FTP server, and a Domain Name System server. This is all controlled via an easy to use graphical user interface directly on the JANUS console. web: http//www.border.com Glenn Mackintosh, Border Network Technologies Inc., 1 Yonge Street, Suite 1400, Toronto, Ontario, Canada, M5E 1J9, Email: glenn@border.com, Tel: +1 416 368 7157, Fax: +1 416 368 7789

Karlbrigde/-Brouter KarlBridge/KarlBrouter - sold by KarlNet Inc in the US and Sherwood Data Systems Ltd in the UK/Europe. Protocol filtering bridge/brouter. The KarlBrouter is identical to the KarlBridge except it provides IP routing (multiple nets per interface - but currently only static routes). The bridge supports filtering of ANY Ethernet protocol and optionally tunnelling within IP and optional encryption. The product also supports protocol filtering of :-

- IP - net/subnet/sockets
- DECnet - net/object0/other objects
- Novell - net/servers/saps/disabling SLIST commands
- AppleTalk - zone/servers/printers/services

There is a shareware/demo (share with colleagues) available from :- ftp://ftp.gbnet.net/pub/kbridge/. WWW: http://www.gbnet.net.kbridge. Available from: Sherwood Data Systems Ltd KarlNet Inc, High Wycombe, UK Columbus, OH, USA, tel (614) 263-KARL, Phone: +44-(0)1494 464264, sales@gbnet.com, sales@KarlNet.com

NetGate NetGate NetGate(TM)is a software firewall for SPARC based systems developed by SmallWorks of Travis Co. SmallWorks specializes in efficient networking utilities and custom software development for SunOS. NetGate was designed to provide routing and filtering for networks of TCP/IP systems without requiring expensive, separately managed hardware. It performs filtering, logging and forwarding for a network or subnetwork of TCP/IP based computers. The extensible rules based system allows the administrator to customize the firewall to allow or

	disallow packets into the network system. NetGate is available for SunOS 4.1.X as either a binary installation, or in source code for the truly adventurous. A single binary license is $1500. Source Code is $2500. Site, corporate-wide and distributor licensing are also available. Send email to: info@smallworks.com. Or telephone/fax to: 512 338 0619
Netpartners	Netpartners: hardware + software. E-Mail: sales@netpart.com
Netra Server	Netra Server by Sun (SMCC)
NetSP	NetSP - IBM. NetSP Secured Network Gateway for AIX is a firewall that runs on any standard IBM Risc System/6000 computer with AIX 3.2.5. - Applications gateways will be provided for telnet and ftp. Users in the protected network log in to the Firewall to use these gateways. The administrator can control which users have access to each of the gateways. - Filtering is the technique of limiting Firewall traffic based on the standard TCP/IP header information of the packets. Filters rules can be based on source and destination address, protocol (TCP, UDP, or ICMP), port number (identifies application), and acknowledgement status (does this packet open a new connection). Phone: 919-254-7416 or 919-254-6898. Fax: 919-254-4239. E-mail: sbaumann@vnet.ibm.com
Network-1	Network-1 Software and Technology, Inc. Network-1 Software and Technology, Inc., who take pride in having Bill Hancock on their staff. Bill told me theirs will be an "inexpensive" offering, meant to "correct" the other overpriced items on the market. He estimated delivery by Q1 ’95. If you’d like to contact them try (800) NETWRK1, or hancock@network-1.com.
Novix	Novix by FireFox (Novell only) IP gateway, partial solution. Brittish company,can function as a firewall for sites with Novell clients. Firefox is an NLM (Netware Loadable Module) which gateways between IPX and TCP/IP.The NLM on the server controls who can get the clients when, etc., and also limits the number of simultaneous users–a form of use-base licensing. Five users cost under $2000, with the price descending to under $300/per simultaneous user. 800 230 6090.
PORTUS	PORTUS by LSLI (Livermore SW Labs). PORTUS is a secure firewall system which represents the state of the art in securing a network from unauthorized intrusions. This software was initially developed at the IBM Thomas J. Watson Research Center in 1988. The PORTUS firewall system provides access from a secure internal network to an unsecured external network without undue hassle. It provides Telnet and File Transfer Protocol (FTP) services to and from the outside world for authorized individuals without compromising network security. PORTUS for the RS/6000 significantly increases the physical security of your valuable data as well as allowing easy access to the Internet. Company Contact Info: 1-800-240-5754. Email: portusinfo@gw.lsli.com. Product support at: portus@gw.lsli.com. Reseller Contact Info: PENTA Inc., 333 North Sam Houston Parkway East, Suite 680, Houston, TX

	77060. Phone: (800) PENTA-79, (713) 999-0093. Fax: (713) 999-0094. E-Mail: penta@phoenix.phoenix.net
Quiotix	Quiotix, jbs@Quiotix.com
SEAL	SEAL - Digital's Firewall Service December 12th _INFOWORLD_ "For more than a decade, the Screening External Access Link, or SEAL, has kept Digitial Equipment's mammoth EasyNet completely impervious to outsiders". SEAL page: http://www.digital.com. FTPable documents : ftp://ftp.digital.com/pub/Digital/info/document/firewall*.*, United States Contact: Dick Calandrella at 508-496-8626
SecurityGate	SecurityGate by DEC >From Dave Church: dave.church@vbo.mts.dec.com PRODUCT NAME: DEC SecurityGate for OpenVMS[*], Version 1.1 SPD DEC SecurityGate software is a VMS software product that, when installed on a DECnet Phase IV routing node, provides an additional level of ac- cess control to that part of the network served by the routing node. A system or security manager can use the DEC SecurityGate software to create a security domain consisting of a group of nodes serviced by the router. HARDWARE REQUIREMENTS: Processor and/or hardware configurations as specified in the System Support Addendum (SSA 36.20.01-x). A TK50 tape drive is required for standalone MicroVAX 2000 and VAXstation 2000 systems
Sidewinder	Sidewinder by SCC (Secure Computing).

Disclaimer: This information comes from sources that cannot be verified. As such, make no assumptions about its completeness or accuracy. I endeavor to keep this list up to date as much as possible. Feel free to send comments/ updates to Catherine Fulmer. Date last update: 02-15-95.

13.4 Resellers & other FW-related Services/products[11]

Maintained by Catherine Fulmer

AlterNet — AlterNet: AlterNet is now offering security consulting services. Bob Stratton Voice) +1 703 204 8000 UUNET Technologies, Inc. Email: strat@uunet.uu.net

Bell Atlantic — Bell Atlantic Network Integration also provides firewall design services.

Data Privacy Facility — Data Privacy Facility - Network Systems

ISS — ISS, Internet Security Scanner, is an auditing package that is publicly available that checks domains and nodes searching for well-known vulnerabilities and generating a log for the administrator to take corrective measures. The publicly available version is on aql.gatech.edu /pub/security/iss.

JANUS — JANUS resellers: **** NetPartners (Phil Trubey) Phone: 800-723-1166, 714-252-5493 Fax: 714-759-1644 EMail: sales@netpart.com **** Sea Change Corporation 6695 Millcreek Drive, Unit 8 Mississauga, Ontario, Canada L5N 5R8 Tel: 905-542-9484 Fax: 905-542-9479 Internet: jalsop@seachange.com WWW: www.seachange.com **** Sea Change Corporation Europe Ltd 470 London Road Slough Berks SL3 8QY UK Phone: 44-1753-581800 Fax: 44-1753-581501 Internet: peter@sea-europe.co.uk WWW: www.sea-europe.co.uk **** Network Translation Services Our company, Network Translation, Inc., has such a Network Address Translation product (see RFC-1631). Give us a call, or check our web site: www.translation.com John Mayes Network Translation, Inc. 415/494-NETS

Stalker — Stalker by Haystack Labs, Inc. intrusion detection system.

Tripcom — Tripcom Systems Inc., reseller for CheckPoint's FireWall-1 product in the Chicago area. Also complete consulting and implementation services for Internet connectivity. An additional product now offered is Livingston's firewall router - IRX. Tripcom Systems Inc. Naperville, IL 708-778-9531 E-Mail: Adam Horwitz

Disclaimer: This information comes from sources that cannot be verified. As such, make no assumptions about its completeness or accuracy. I endeavor to keep this list up to date as much as possible. Feel free to send comments/ updates to Catherine Fulmer. Date last update: 02-15-95.

[11] Vergleiche aktuell: [Fulmer,C.]

13.5 Stichwortverzeichnis[12]

Glossary of Terms

Abuse of Privilege	When a user performs an action that they should not have, according to organizational policy or law.
Application-Level Firewall	A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.
Authentication	The process of determining the identity of a user that is attempting to access a system.
Authentication Token	A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.
Authorization	The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.
Bastion Host	A system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., UNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.
Challenge/Response	An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.
Chroot	A technique under UNIX whereby a process is permanently restricted to an isolated subset of the filesystem.
Cryptographic Checksum	A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting filesystem tampering on UNIX.
Data Driven Attack	A form of attack in which the attack is xencoded in innocuous-seeming data which is executed by a xuser or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get

[12] Entnommen aus: [Ranum,M.-4]

	through the firewall in data form and launch an attack against a system behind the firewall.
Defense in Depth	The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.
DNS spoofing	Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.
Dual Homed Gateway	A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.
Encrypting Router	see Tunneling Router and Virtual Network Perimeter.
Firewall	A system or combination of systems that enforces a boundary between two or more networks.
Host-based Security	The technique of securing an individual system from attack. Host based security is operating system and version dependent.
Insider Attack	An attack originating from inside a protected network.
Intrusion Detection	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.
IP Spoofing	An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.
IP Splicing / Hijacking	An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.
Least Privilege	Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.
Logging	The process of storing information about events that occurred on the firewall or network.
Log Retention	How long audit logs are retained and maintained.
Log Processing	How audit logs are processed, searched for key events, or summarized.
Network-Level Firewall	A firewall in which traffic is examined at the network protocol packet level.

Perimeter-based Security	The technique of securing a network by controlling access to all entry and exit points of the network.
Policy	Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.
Proxy	A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
Screened Host	A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.
Screened Subnet	A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.
Screening Router	A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.
Session Stealing	See IP Splicing.
Trojan Horse	A software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program.
Tunneling Router	A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual deencapsulation and decryption.
Social Engineering	An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems.
Virtual Network Perimeter	A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks.
Virus	A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

13.6 Literatur

Avolio,F.M.	Firewalls Are Not Enough, Data Security Letter, Number 50
Barkley,J.	Security in Open Systems, NIST Special Publication 800–7, http://csrc.ncsl.nist/nistpubs, Feb. 1995
Bellcore	S/Key Authentication, ftp://ftp.leo.org/pub/comp/os/bsd/FreeBSD/FreeBSD–current/src/lib/libskey, Jun. 1995
Bellovin,S.-1	Firewall-Friendly FTP, AT&T Bell Laboratories, RFC 1579, Feb. 1994
Bellovin,S.-2	Security Concerns for IPng, AT&T Bell Laboratories, RFC 1675, Aug. 1994
Bellovin,S.-3	Security Problems in the TCP/IP Protocol Suite, AT&T Bell Laboratories, Computer communications Review Vol.19, No.2, pp32–48, April 1989
Bryan,J.	Build a Firewall, Firewalls for Sale, Byte Magazine, April 1995
Carl-Mitchell, Quarterman	Building Internet Firewalls – Tutorial, UNIXWORLD, Feb. 1992
Chapman, Zwicky	Building Internet Firewalls, O'Reilly & Associates, 1st Edition, ISBN 1–56592–124–0, Sept. 1995
Chapman,D.B.	Network (In)Security Through IP Packet Filtering, Great Circle Associates, Mountain View, CA, Published in *Proceedings of the Third USENIX UNIX Security Symposium*, Baltimore, MD, Sep. 1992
CERT	Cert Advisory — IP Spoofing Attacks and Hijacked Terminal Connections, CA-95:01, Jan. 23 1995
Cheswick,B.	The Design of a Secure Internet Gateway, AT&T Bell Laboratories,
Cheswick, Bellovin	Firewalls and Internet Security – Repelling the Wily Hacker, Addison-Wesley Professional Computer Series, ISBN 0–201–63357–4, Jul. 1994
Cisco	Cisco IOS Security Architecture, 1995
DEC-1	Internet Security: Screening External Access Link (SEAL), http://www.digital.com, Jan. 1995
DEC-2	Digital's Firewall Service — Introductory Guide, DEC, Maynard, Massachusetts, Aug. 31 1994
Dalva,D.I.	Security and the World Wide Web, Trusted Information Systems, Inc., http://www.tis.com, Aug. 12 1994

DeSchon,A. Cohen,D.	The ISI “Tunnel”, USC Information Sciences Institute, Okt. 12 1993
Dieth,Haug,Kienle,Heinen	Report Netzwerksicherheit – Marktübersicht: Kommerzielle Firewalls — Katz und Maus, iX 9/1995
Ellermann,U. – 1	Firewalls — Klassifikation und Bewertung, Fachbereich Informatik, Universität Hamburg, DFN-Bericht 75, Mär. 3 1994
Ellermann,U. – 2	Firewalls — Isolations- und Audittechniken zum Schutz von lokalen Computer-Netzen, DFN-CERT, Fachbereich Informatik, Universität Hamburg, DFN-Bericht 76, Sep. 1994
Fischer,D.	Sicherheit im Internet, GAI NetConsult GmbH, Berlin
Fulmer,C.	Commercial Firewalls and partial FW products, Resellers & other FW-related Services/products, http://www.digimark.net/bdboyle/fulmer/firewall.vendor.html, Feb. 15, 1995
IBM-1	IBM NetSP Secured Network Gateway for AIX — A reliable firewall between your network and the Internet, or any network, G325–3456–00, Nov. 1994
IBM-2	IBM NetSP Secured Network Gateway V1.2. Announcement Letter No. ZP94–0793, Dez. 6 1994
IBM-3	IBM NetSP Secured Network Gateway V1.2. Installation, Configuration and Administration Guide, SC31–8113–00, First Edition, Dez. 1994
Kienle,M.	Standhafte Mauern, Sicherheit für lokale Netze ohne Diensteinschränkung, iX 7/1994
Klute,R.	Zwischenstation, Mit dem Proxy-Server Zeit und Geld sparen, iX 2/1995
Koblas,D., Koblas,M.	SOCKS, USENIX Security Symposium III, 1992
Livingston Enterprises Inc.	FireWall Application Notes, Livingston Enterprises Inc., Part No. 950–1142A, Jul. 1994
Luotonen,A. Altis,K.	World-Wide Web Proxies, CERN, Intel, Apr. 1994
Mogul,J.	Using screend to Implement IP/TCP Security Policies
Morris,R.T.	A Weakness in the 4.2 BSD Unix TCP/IP Software, AT&T Bell Laboratories, Feb. 25 1985
NIST-1	Computer Security Publications — NIST Publication List 91, NIST, http://csrc.ncsl.nist/nistpubs, Okt. 1994
NIST-2	Management Guide to the Protection of Information Resources, NIST, http://csrc.ncsl.nist/nistpubs, Feb. 1995
Polk,W.T.	Automated Tools for Testing Computer System Vulnerability, NIST, http://csrc.ncsl.nist/nistpubs, Dez. 3, 1992
Ranum,M.-1	A Network Firewall, DEC Washington Open System Resource Center, Greenbelt, MD, Jun. 12 1992

Ranum,M.-2	Internet Firewall Protection – Tutorial,, Open Computing, Sep. 1994
Ranum,M.-3	Thinking About Firewalls, ftp://ftp.greatcircle.com, /pub/firewalls/papers/ranum
Ranum,M.-4	Firewall Product Functional Summary, Information Warehouse Inc., ftp://ftp.iwi.com, Aug. 1995
Ranum,M., Avolio	A Toolkit and Methods for Internet Firewalls, Teil der Dokumentation, http://www.tis.com, Jan. 1995
Reinhardt,R.B.-1	An Architectural Overview of UNIX Network Security, ARINC Research Corporation, Annapolis, Feb. 18 1993
Reinhardt,R.B.-2	An Architectural Overview of UNIX Network Security, (Specifically oriented toward Internet connectivity), Sep. 19 1992
RFC-812	NICNAME/WHOIS, K.Harrstien,, M.Stahl, E.Feinler, Okt. 1985
RFC-1288	The Finger User Protocol, D.Zimmermann, Center for discrete Mathematics and Theoretical Computer Science, Dez. 1991
Robinson, A.T.	INTERNET FIREWALLS – An Introduction, Revision 235, netMAINE, Jul. 19 1994
Safford, Schales, Hess-1	The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment, Supercomputer Center, Texas A&M University, College Station, TX, Published in *Proceedings of the Fourth USENIX Security Symposium*, 1993
Safford, Schales, Hess-2	Texas A&M Network Security Package Overview, Beta Release 1.0, David-Hess@tamu.edu, Jan. 1995
Safford, Schales, Hess-3	Texas A&M Drawbridge 2.0 Beta, TAMU Computing and Information Services – Network Group, David-Hess@tamu.edu, Feb. 1 1994
SecurID	Security Dynamics – Securing the Information Age ... Minute by Minute, Security Dynamics Technologies, 101A4 20M 4/1/95
SUN	FireWall-1 1.0 Internet Security Software, SunFlash 71.45, ftp://nic.uakom.sk, Dez. 1994
Treese,G.W., Wolman,A.	X Through the Firewall, and Other Application Relays, DEC Cambridge Research Laboratory, Technical Report Series, Mai 03 1993
TIS-1	Gauntlet – The Internet Firewall from Trusted Information Systems Inc., http://www.tis.com, Jan. 1995
TIS-2	TIS Firewall Toolkit, Teil der Dokumentation, http://www.tis.com, Jan. 1995

TIS-3	TIS Firewall Toolkit Overview, Teil der Dokumentation, http://www.tis.com, Jan. 1995
Varadhan,K.	OARnet Security Procedures, OARnet engineering group, OARnet, Columbus, OH, Sep. 15 1992
Venema,W.	Wietse's tools and papers, available by e-mail, wietse@wzv.win.tue.nl
Vinzencetti,D.	STEL: Secure TELnet, Fifth USENIX Unix Security Symposium, Salt Lake City,UT, June 1995
Wack,J.P., Carnahan,L.J.	Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, NIST, Draft Nov. 30 1995
Winkler,I.S., Dealy,B.	Information Security Technology?... Don't Rely on It — A Case Study in Social Engineering, Proceedings of the Fifth USENIX Unix Security Conference, Salt Lake City, UT, ISBN 1–880446–70–7, Jun. 1995